Afstudeerscriptie

Monitoring

Een onderzoek naar het verhogen van het cybersecurityvolwassenheidsniveau door monitoring bij Koninklijke Oosterberg B.V.

KONINKLIJKE OOSTERBERG

Student	Bart Franck 448454@student.saxion.nl Bart.franck@oosterberg.nl
Project	Monitoring, logging & events
Academie	Academie Creatieve Technologie
Betrokken partijen	Saxion Hogeschool Enschede Koninklijke Oosterberg B.V.
Afstudeerbegeleider(s)	Dhr. F. Bouwman Dhr. R. Bourgonje
Afstudeerdocent	Drs. E.M. Hageraats
Datum	13-06-2021
Versie	1.1

Voorwoord

Voor u ligt de scriptie van Bart Franck, studerende aan het Saxion College te Enschede en afstudeerder bij Koninklijke Oosterberg B.V. Deze scriptie is een samenvoeging van de gemaakte documenten gedurende het afstudeertraject over het verhogen van het beveiligingsvolwassenheidsniveau door het toepassen van monitoring. Deze afstudeerperiode is ontzettend leerzaam geweest en heb ik ervaren als een leuke en leerzame uitdaging.

Middels deze weg wil ik graag mijn begeleiders en collega's van Oosterberg bedanken voor hun bijdrage aan mijn afstudeerscriptie. De fijne collegiale sfeer maakt het dat ik altijd terecht kan voor vragen en input.

Daarnaast bedankt ik ook graag de opleiding Information Technology Service Management (ITSM) voor de leerzame en interactieve lesjaren waarin ik zowel op technisch als persoonlijk gebied enorm ben gegroeid. Tot slot bedank ik graag Esther Hageraats voor de zeer prettige communicatie en begeleiding tijdens dit afstudeertraject, waarbij ik in het bijzonder ook Ruud Greven wil noemen en bedanken als fantastische studieloopbaanbegeleider.

Versieoverzicht

Versie	Datum	Wie	Wijziging
0.1	11-02-2021	Bart Franck	Document aangemaakt & lay-out toegevoegd
0.2	03-03-2021	Bart Franck	Herinrichting van de structuur
0.3	13-04-2021	Bart Franck	Herinrichting van de structuur
0.4	13-05-2021	Bart Franck	Herinrichting van de structuur & verwerken feedback v0.3
0.5	26-05-2021	Bart Franck	Herzien structuur a.d.h.v. feedback v0.4
1.0	30-05-2021	Bart Franck	Afronding scriptie i.v.m. conceptuele oplevering
1.1	13-06-2021	Bart Franck	Definitie afronding scriptie

Tabel 1 Versiebeheer

Distributielijst

Versie	Datum	Wie	Aan
0.3	29-04-2021	Bart Franck	Esther Hageraats
1.0	30-05-2021	Bart Franck	Esther Hageraats, Mevlit Akca
1.1	13-06-2021	Bart Franck	Esther Hageraats, Mevlit Akca

Tabel 2 Distributiebeheer

Definities

Afkorting	Definitie
ISCM	Information Security Continuous Monitoring
SIEM	Security Information and Event Management
WMI	Windows Management Instrumentation
CVE	Common Vulnerabilities and Exposures
DLP	Data Loss Prevention
KPI	Key Performance Indicator
SNMP	Simple Network Management Protocol
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
DMZ	Demilitarized zone
LMS	Log Management System
SEM	Security event manager
SIM	Security information management
SEC	Security event correlation
CSO	Chief security officer
CISO	Chief information security officer
LUN	Logical Unit Number

Tabel 3 Definitiebeheer

Managementsamenvatting

Koninklijke Oosterberg wil haar beveiliging op een hoger volwassenheidsniveau krijgen. Om een start te maken aan het verhogen van dit niveau heeft Oosterberg een assessment door ICT-Security bedrijf Fox-IT laten uitvoeren. Dit security assessment toont aan dat er diverse onderdelen zijn die binnen de organisatie opgepakt kunnen worden. Een van deze onderdelen is het op goede wijze inrichten van monitoring.

Oosterberg wil daarom monitoring op centrale en optimale wijze in te zetten. Het primaire doel is om risicomanagement op te pakken om zo businesscontinuïteit te garanderen. Hierbij dient het mogelijk te worden voor Oosterberg om weer meer in controle te komen over haar eigen infrastructuur en ICT-omgeving. Dit dient behaald te worden door inzicht in logging en events, door trends te kunnen analyseren, correleren en rapporteren en op gebruiksvriendelijke en centrale wijze deze data te kunnen gebruiken.

Uit onderzoek blijkt dat monitoring veel dimensies kent, waarbij er onder andere onderscheid gemaakt wordt tussen strategieën, protocollen en standaarden. Deze onderdelen kunnen gevolgd en ingezet worden om herleidbaar en verantwoord monitoring in te richten. Daarnaast is log management het begrip dat veelal wordt gebruikt om monitoring te beschrijven. Dit komt omdat log management onderverdeeld wordt in monitoren, loggen en rapporteren. Het onderzoek beschrijft dat al deze aspecten ingezet kunnen worden om monitoring op een hoger niveau te krijgen, waarbij een belangrijk uitgangspunt is dat het middels best practices wordt gedaan. Dit komt overeen met de wensen van Oosterberg: om het op optimale wijze te doen. Deze best practices beschrijven dat een Top-down approach het beste toegepast kan worden bij monitoring projecten, omdat dit ertoe leidt dat zowel ICT-afdeling, de techniek en businessprocessen op een lijn komen te zitten. Monitoring dient tenslotte ingezet te worden om de businesscontinuïteit te garanderen. Businesscontinuïteit kan gegarandeerd worden op het moment dat de organisatie veilig is en er geen beveiligingslekken ontstaan, waardoor de continuïteit stilvalt.

Door het gehele project heen kan gesteld worden dat er twee opties beschikbaar zijn voor Oosterberg. In het geval van een technische oplossing wordt er gesproken over het toepassen van een Log Management System (LMS) of een Security Information and Event Managementsysteem (SIEM). De eisen en wensen van Oosterberg passen het beste bij het toepassen van een SIEM-oplossing, waarbij het van belang is dat de juiste oplossing geselecteerd wordt. Om tot de juiste oplossing te komen wordt er een multi criteria decision analyse uitgevoerd. Deze selectiemethode berekend welke SIEM-tool het beste bij Oosterberg past en doet dit op basis van criteria met een relevantiegewicht. Uit deze analyse blijkt dat Splunk (Enterprise Security) goed aansluit bij Oosterberg. Uit onderzoek blijkt wel dat SIEM-oplossingen in gewenste situaties geïmplementeerd worden door een partner. Uit SIEM-best practices blijkt ook dat het beheren van een SIEM-oplossing het beste gedaan kan worden door securityspecialisten, analisten of Security Operation Center (SOC) medewerkers. Bij Oosterberg is hier momenteel niet de benodigde tijd of capaciteit voor. Dit leidt tot het advies dat het implementeren en beheren van Splunk Enterprise Security beter uitbesteed kan worden. Hierdoor krijgt Oosterberg een kennisvolle partner waarmee samengewerkt kan worden, leidt dit ertoe dat er volgens best practices wordt gewerkt, dat er minimale impact is op de businessprocessen en dat een technische oplossing tot in volledigheid wordt gebruikt.

Tot slot blijkt uit onderzoek ook dat gedragsanalyse van gebruikers, systemen en het inzien van rechtenwijzigingen op accounts en bestanden onder de functionaliteiten van UEBA vallen. UEBA staat voor User Entity Behavior Analysis en het blijkt dat veel leveranciers deze functionaliteit niet standaard in een SIEM-oplossing hebben zitten. Splunk levert hier een andere oplossing voor, namelijk Splunk UBA. Deze oplossing kan naadloos geïntegreerd worden met Splunk Enterprise Security (SIEM) op het moment dat deze wens er is. Deze samenvoeging werkt pas optimaal als Splunk Enterprise Security een langere periode geïntegreerd is.

Inhoudsopgave

Figuuropgave:

Tabelopgave:

1 Inleiding

Voor u ligt de scriptie van Bart Franck, in opdracht van Koninklijke Oosterberg B.V. Deze afstudeerscriptie is een onderzoek naar het (her)inrichten van monitoring bij Oosterberg en op welke wijzen dit gedaan kan worden. Door het inzetten van monitoring wil Oosterberg haar eigen omgeving en infrastructuur meer onder controle zien te krijgen, waarbij het doel is om een stuk risicomanagement te kunnen oppakken. Hiermee probeert Oosterberg op een hoger beveiligingsvolwassenheidsniveau te komen.

De scriptie is een ingekorte versie van meerdere documenten en heeft een maximale grootte van 49 pagina's, dit is exclusief bijlagen en reflectie. De scriptie zal de lezer meenemen in de belangrijkste aspecten van dit project. De indeling van de scriptie luidt als volgt:

Achtergrond
Dit hoofdstuk levert informatie over Oosterberg en over de totstandkoming van het project.
Methodieken
Dit hoofdstuk levert informatie over de gebruikte methoden en methodieken binnen dit project
Probleemanalyse
Dit hoofdstuk brengt het probleem met bijbehorende oorzaken in kaart en wordt geconcludeerd in hoofd- en deelvragen.
Vooronderzoek
Dit hoofdstuk bestaat uit de behoefteanalyse en contextanalyse, waarbij de behoefteanalyse bouwt op de probleemanalyse en concludeert in de eisen en wensen van Oosterberg. De contextanalyse concludeert in randvoorwaarden en bouwt verder op de behoefteanalyse. De huidige situatie wordt hier ook inzichtelijk gemaakt.
Literatuuronderzoek
Dit hoofdstuk betreft een onderzoek naar conceptuele oplossingen en concludeert in ontwerpprincipes, die als aanleiding voor het ontwerp dienen.
Ontwerp
Het ontwerp wordt gestart met een stuk onderzoek in de vorm van een pakketselectie (multi criteria decision analysis). Het ontwerp bestaat uit een functioneel en technisch ontwerp, waar vorm wordt gegeven aan de haalbare oplossingen en hoe deze inspelen op de casus van Oosterberg.
Eindevaluatie
De eindevaluatie beschrijft de resultaten en concludeert de scriptie in de vorm van aanbevelingen.

2 Achtergrond

De organisatie

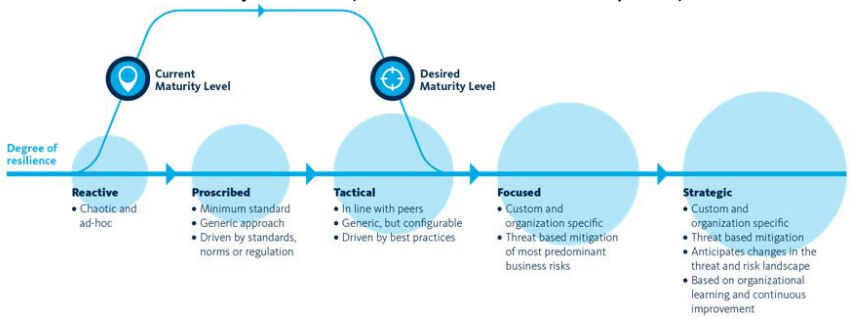
Oosterberg een van de grootste elektrotechnische groothandels van Nederland. De elektronische producten die geleverd worden komen uit een groot assortiment en betreft producten zoals kabels, buizen, schakelaars, installatiekasten, verlichting, industriële componenten en nog veel meer. Oosterberg is een familiebedrijf en probeert zich in de markt te onderscheiden met haar service en diensten. Kort door de bocht is het doel simpel, zo veel mogelijk producten verkopen, maar dan wel door de organisatie te laten uitblinken in de markt en dit op een juiste wijze doen. Oosterberg levert naast elektronische producten ook op maat gemaakte oplossingen. Het is een snelgroeiend bedrijf met meer dan 400 medewerkers, verspreid over 21 vestigingen in heel Nederland. De ICT-afdeling heeft op het moment dat dit geschreven wordt 9 medewerkers met 2 openstaande vacatures en 2 ingehuurde krachten. Het afstudeerproject wordt thuis uitgevoerd i.v.m. COVID-19 en op de hoofdlocatie in Apeldoorn, waar zo'n 50 medewerkers werken.

Missie en visie

"Oosterberg gelooft dat grootschaligheid wel degelijk samen kan gaan met persoonlijk contact en flexibiliteit. We investeren in relaties en brengen daarmee de wensen en behoeften van de markt in kaart. Onze producten en diensten passen we daarop aan. Het succes van Oosterberg is nauw verbonden met het succes van onze klanten en leveranciers, daar zijn we van overtuigd. Wederzijdse afhankelijkheid zien wij als kracht die we willen omarmen en ten volle benutten. Dit is essentieel voor het voortbestaan van ons allen op de lange termijn" (Oosterberg, 2021).

Aanleiding en context

Oosterberg heeft op 27-05-2020 ervoor gekozen om het hele beveiligingsbeleid op een hoger niveau te krijgen. Hiervoor is contact opgenomen met het security-gespecialiseerd ICT-bedrijf Fox-IT, om vanuit hun specialisme hier advies over te krijgen. Na diverse contactmomenten met Fox-IT, is er een 'Architectuur Review' uitgevoerd ten aanzien van de inrichting van cybersecuritycomponenten en processen binnen de organisatie van Oosterberg. Er zijn toen 16 bevindingen opgenomen in het rapport, met diverse risico classificaties. Het uitgangspunt van deze Architectuur Review is dat Oosterberg ervoor gaat zorgen dat het bedrijf op een hoger beveiligingsvolwassenheidsniveau komt. Zo zal de afdeling Automatisering weer meer in controle zijn over haar infrastructuur en de bedrijfsdata. Sinds dien is de automatiseringsafdeling druk bezig om een beleid/ plan op te stellen en om daarnaast tegelijkertijd bezig te zijn met het verbeteren van de volwassenheid omtrent infrastructuurbeveiliging. Onderstaande afbeelding geeft aan op welk niveau Oosterberg zat ten tijde van de Architectuur Review en waar het bedrijf heen wil (current en desired maturity level).



Figuur 1 Cybersecurity Maturity Level Fox-IT (Bresser, 2020)

Veel van deze 16 bevindingen zijn al opgenomen of zijn momenteel in behandeling, maar een van de meest belangrijke onderdelen staat nog op de planning: Het centraliseren van logging en het uitbreiden van monitoring. Het centraliseren van logs en de monitoring wordt geclassificeerd als punt M06 in het rapport en heeft een hoge prioriteit.

ID	Prio	Mitigerende maatregel	Relatie naar bevindingen
M06	!!	**Richt logging en monitoring in** – Stel beleid op voor logging – Regel monitoring breed in voor de volledige technologie stack – Centraliseer logging (SIEM) – Log en activeer alerting	AR10, AR01

Figuur 2 Logging en Monitoring - M06 (Bresser, 2020)

Fox-IT geeft aan dat een SIEM-oplossing de organisatie naar een hoger beveiligingsvolwassenheidsniveau kan brengen. SIEM is een Security Information en Event Management tool, waarmee netwerkactiviteiten gevolgd en getraceerd kunnen worden. SIEM-tools staan vaak als fundament in een sterke IT Security-omgeving.

Monitoring wordt opgebroken in logging & events, rapporteren en het monitoren van de gehele infrastructuur.
Risicomanagement is het primaire doel i.v.m. het willen beschermen tegen dreigingen, forensisch onderzoek willen uitvoeren en het willen bewaken van de integriteit en beschikbaarheid (businesscontinuïteit) van de infrastructuur. Het organisatiebelang bij deze opdracht luidt daarom als volgt:
'Oosterberg wil de betrouwbaarheid, integriteit en beschikbaarheid van de IT-systemen en infrastructuur kunnen garanderen, omdat businesscontinuïteit voorop staat'.

3 Methodieken

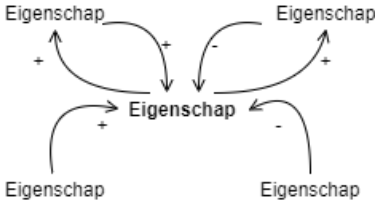
Het schrijven van een onderzoek/ scriptie kan het beste worden uitgevoerd door diverse methodieken toe te passen. Door gebruik te maken van verschillende technieken en methoden kan informatie op juiste wijze genoteerd en herleid worden. Tijdens de afstudeerperiode zijn er diverse methodieken gebruikt om tot verschillende conclusies te komen. Het gebruiken van de juiste methode bij de verschillende onderdelen, zal ertoe leiden dat alles duidelijk en helder geformuleerd wordt. In dit hoofdstuk worden de gebruikte methodieken toegelicht.

Ontwerponderzoek
Het project met daarbij de onderzoek en ontwerpfase wordt uitgevoerd door gebruik te maken van de methodiek 'Ontwerponderzoek'. Deze methodiek wordt gehanteerd om te garanderen dat het een wetenschappelijk verantwoord onderzoek is, die resulteert in een ontwerp voor een interventie of een directe interventie waarmee een concreet probleem kan worden opgelost (Haveman, Hageraats, & Linden, 2016).

Stakeholder analyse
Een stakeholderanalyse wordt toegepast om de belangrijkste spelers binnen dit project in kaart te brengen. Zo kan er goed ingespeeld worden op de verschillende belanghebbenden en hun perspectieven. De stakeholderanalyse wordt uitgevoerd d.m.v. de matrix van Mendelow (Eriksen-Coats, 2018). Hierin wordt er per belanghebbende (stakeholder) bepaald hoeveel interesse (belang) en macht deze heeft. De belanghebbenden met hoge macht en interesse zijn de key-players tijdens het project.

Root cause analyse
Het in kaart brengen van problemen en de oorzaak/ oorzaken wordt gedaan door een root cause analysis uit te voeren. Door dit model toe te passen op de problemen die worden ervaren, kan er geanalyseerd worden wat de 'root-oorzaken' zijn van de verschillende geschetste en benoemde problemen (Sigma Groep, 2021). Er is gekozen om deze methodiek toe te passen om zo per perspectief helder en herleidbaar de problemen en oorzaken in kaart te kunnen brengen.

Causalerelatiediagram
Het in kaart brengen van eigenschappen van iets dat verduidelijkt moet worden, wordt gedaan door het causale relatiediagram. Dit model/ diagram beschrijft hoe eigenschappen in de omvang van het project elkaar beïnvloeden. De keuze om dit model uit te werken is omdat alle mogelijke gevolgen en relaties zo in kaart worden gebracht.



Figuur 3 Causaal relatiediagram voorbeeld

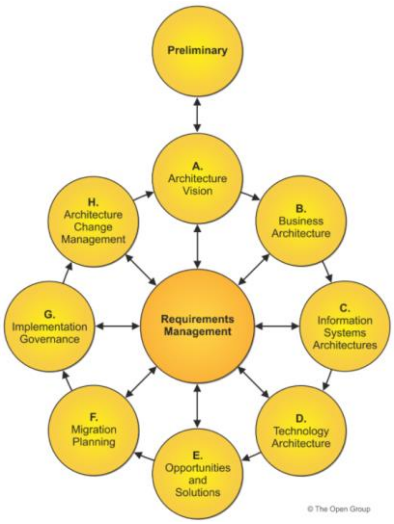
- Een pijl A —+→ B betekent "als A in waarde toeneemt neemt B ook in waarde toe", en ook "als A in waarde afneemt neemt B ook in waarde af".
- Een pijl A – – → B betekent "als A in waarde toeneemt neemt B juist in waarde af", en ook "als A in waarde afneemt neemt B juist in waarde toe" (TU Delft, 2020).

Verander kaleidoscope
Deze methodiek kan ook als model worden gezien. Dit model heeft een aantal dimensies waarin op verschillende onderdelen worden ingeschat en bepaald wat de veranderaspecten zijn tijdens en na afronding van een project. De organisatie verander context (de buitenring) wordt allereerst tekstueel beschreven, waarna er wordt ingedoken op de middenlaag, waarna tot slot de binnenste cirkel wordt uitgewerkt. Er wordt onder andere gekeken naar de beschikbare tijd, autonomie en beschikbaarheid van medewerkers, geld en de gereedheid van betrokken belanghebbenden.
De verander kaleidoscope zorgt voor het in kaart brengen van een brede omvang van contextuele toepassingen en implementatiemogelijkheden, die potentieel veranderd gaan worden en daarom overwegen zullen moeten worden. Het model behandeld acht onderdelen, namelijk: Time, Scope, Preservation, Diversity, Capability, Capacity, Readiness en Power (Muravu, 2020). Er is gekozen voor dit model/ deze methodiek om alle mogelijke aspecten te behandelen en de organisatiecontext zo breed mogelijk in kaart te brengen. Zo wordt er niets achterwege gelaten.

GAP-analyse
De GAP-analyse wordt gedeeltelijk uitgewerkt in de contextanalyse. In deze GAP-analyse worden de huidige probleemsituatie (IST) en gewenste situatie (SOLL) in kaart gebracht. De IST-situatie wordt uitgevoerd voor het vooronderzoek tijdens de contextanalyse. De SOLL-situatie wordt in het technisch ontwerp uitgewerkt. Er is gekozen om deze twee situaties uit te werken om op strategisch niveau aan te kunnen tonen wat mogelijke veranderingen zijn die de organisatie op kan pakken in een gewenste situatie (Boer, 2015).

ArchiMate
De modelleertaal van ArchiMate wordt gebruikt om Enterprise architecturen in kaart te brengen. Het zal ingezet worden om concepten en relaties tussen verschillende architectuurdomeinen inzichtelijk te maken. Het doel van ArchiMate is om op simpele wijze te modelleren waar eventuele knelpunten zitten, terwijl er wordt voorkomen dat elk mogelijk scenario in kaart moet worden gebracht. ArchiMate maakt gebruik van een drielagen-model, waarbij de lagen geclassificeerd worden als Business, Application en Technology.

TOGAF
De TOGAF-standaard geeft richtlijnen en biedt als het ware een framework om (Enterprise) architecten op een herleidbare en flexibele manier, verschillende soorten architectuurstijlen toe te laten passen. TOGAF is een high-level ontwerpaanpak en is vooral afhankelijk/ gebaseerd op standaardisatie van bestaande, bewezen technologieën en producten. TOGAF kan zorgen dat de business efficiëntie wordt verhoogd. Het framework zorgt voor een aanpak om ontwerpen, planning, implementatie en governance op een strategisch, high-level niveau toe te passen. TOGAF zal worden toegepast omdat de juiste architectuurprincipes en methodieken zo worden gebruikt. Er wordt gekozen om TOGAF toe te passen door deze strategische en high-level aanpak (Opengroup, 2021).



Figuur 4 TOGAF-framework

UML
Het uitwerken en beschrijven van resultaten van requirements, systeemstructuur en gedrag van het systeem wordt gedaan door UML-diagrammen uit te werken. De mogelijke scenario's en alle objectrelaties worden door deze activity, class of bijvoorbeeld sequence diagrammen uitgewerkt. Het toepassen van UML wordt in dit project gedaan op basis van een use case, activity diagram en een component diagram. Door UML in te zetten wordt duidelijk wat de koppelingen en relaties zijn tussen verschillende processen en objecten (Fowler, 2003).

MoSCoW
Eisen en wensen vloeien voort uit het voeren van diverse analyses, interviews en gesprekken. Deze eisen en wensen (requirements) zullen gecategoriseerd moeten worden. Dit zal worden gedaan door de MoSCoW-methodiek, waarbij aan wordt gegeven welke requirements 'Must, Should, Could en Won't have' zullen krijgen. MoSCoW is een methode die uit de Agile-projectmethodiek komt. Op deze manier wordt duidelijk waar wel en geen aandacht aan besteden hoeft te worden.

Ontwerpprincipes
Resultaten uit de literatuurstudie zijn ontwerpprincipes. Ontwerpprincipes zijn leidende fundamenten onder het toekomstige ontwerp en zorgen ervoor dat de kennis uit eerdere onderzoeken in de interventie wordt toegepast (Haveman, Hageraats, & Linden, 2016). De ontwerpprincipes hebben de volgende structuur: (alle beschreven ontwerpprincipes voldoen aan deze vormgeving).

ALS, DAN, OMDAT (voorbeeld):
ALS monitoring goed is ingericht DAN kan er beter geanticipeerd worden op mogelijke dreigingen OMDAT uit voorgaande onderzoeken blijkt dat goed monitoren centraal staat in een veilige infrastructuur.

Multicriteria decision analysis
Om te onderzoeken welke technische oplossing het beste bij de organisatie past, wordt de methode 'multicriteria decision analysis' uitgevoerd (MCDA). Het doel van deze analyse is het vergelijken van meerdere oplossingen, terwijl er rekening wordt gehouden met de eisen en wensen van de organisatie, door relevantie te verwerken.
Relevantie & Calculatie:
Bij het opstellen van criteria wordt er rekening gehouden met eisen en wensen, waarbij de gestelde eisen en wensen een gewicht krijgen (weight). De relevantie is vastgesteld a.d.h.v. de eisen en wensen van Oosterberg. Vervolgens kunnen de volgende scores worden toegekend: -3, -2, -1, +1, +2, +3. De totaalscore wordt bepaald door het gewicht * score te berekenen. Hierbij wordt alles in de min geclassificeerd als 0 om zo de berekening accuraat te houden. Dit resulteert in een 'beste oplossing' voor Oosterberg.

4 Probleemanalyse

Inleiding
De probleemanalyse is de eerste stap uit het uit de onderzoeksfase vanuit het ontwerponderzoek. De probleemanalyse geeft antwoorden op de waarom en wat vragen omtrent de mogelijke problematiek. Op het moment dat er uit de probleemanalyse blijkt dat er een daadwerkelijk probleem speelt, probeert deze analyse dit te definiëren. Deze probleemanalyse kan gezien worden als basis, het gehele project zal hiernaar terug worden gerefereerd en zal de informatie die uit deze analyse voortvloeit worden (her)gebruikt. Door deze redenen is het belangrijk dat de probleemanalyse op valide wijze beschreven wordt. De probleemanalyse zal zich uitmonden in hoofd- en deelvragen.

Methoden
Dit onderdeel beschrijft welke methoden er gebruikt worden tijdens de probleemanalyse en waarom deze methoden gebruikt worden.

- Deskresearch – Het onderzoeken van documentatie van Fox-IT en Oosterberg.
- Fieldresearch – semigestructureerde interviews met alle belanghebbenden uit de stakeholderanalyse in de behoefteanalyse.
- Causaal model – Per perspectief noteren wat het probleem is en wat de oorzaken hiervan zijn
- Causale relatiediagram – alle opgehaalde informatie vanuit de interviews en analyses verwerken in een diagram om alle concepten, knelpunten en invloeden in kaart te brengen

Probleemomschrijving
Oosterberg bevindt zich momenteel in een stadium waarbij er een enorme groei is binnen de organisatie. Met de komst van medewerkers dient de infrastructuur mee te schalen en met de komst van alle nieuwe infrastructuurcomponenten wordt het lastiger om alles onder controle te houden. Een belangrijk onderdeel van controle over de infrastructuur, is een goede inrichting van de beveiliging. Hierbij behoort het inzicht in netwerkcomponenten en het analyseren van trends. Deze wensen zijn in recente tijden steeds groter geworden door het toenemende belang bij cyber security. Het belang bij cyber security wordt groter door de toename aan dreigingen van buitenaf, waarbij Oosterberg met name een slachtoffer zou kunnen worden van ransomware. Het voorkomen van incidenten door deze dreigingen is daarbij een belangrijk doel. Een belangrijk uitgangspunt is ervoor zorgen dat het niet langer een reactieve ICT-afdeling is en dat er meer proactief gewerkt gaat worden.

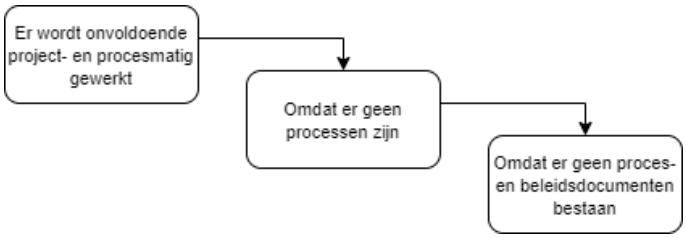
Een betere beveiliging van de infrastructuur door inzicht in data, zoals de logs- en events van netwerkcomponenten, komt ook terug in een security assessment van het bedrijf Fox-IT. Dit assessment bevat verbeterpunten, zodat Oosterberg op een hoger beveiligingsvolwassenheidsniveau terecht kan komen. Een van deze onderdelen is onderzoeken naar hoe monitoring beter kan worden ingericht. Het implementeren van een SIEM-oplossing om logging en events te kunnen centraliseren, analyseren en rapporteren is daarbij een aanbeveling vanuit Fox-IT. Daarbij wil Oosterberg graag weten op welke manier dit het beste gedaan kan worden en op welke verschillende wijze er analyses gedaan kunnen worden.

4.1 Perspectieven

Bepaling perspectieven
Het ophalen van alle (belangrijke) perspectieven wordt gedaan via de brainstorm-methode in combinatie met de belanghebbendenanalyse die uitgevoerd is in de behoefteanalyse. De belanghebbenden worden daar in een longlist opgesomd, waarna het resulteert in een shortlist met de belanghebbenden die de meeste interesse en macht hebben binnen Oosterberg.
Deze perspectieven in kaart brengen zal ervoor zorgen dat het probleem/ de problemen duidelijk in beeld komen en worden beschreven. Het gebruiken van meerdere perspectieven zorgt voor triangulatie, de mogelijke problemen worden zo vanuit meer dan één kant belicht. De resultaten van de stakeholderanalyse zijn in onderstaande opsomming gebruikt en de perspectieven worden afgerond door de toevoeging van zowel de theorie (literatuur) als de onafhankelijke blik van de onderzoeker. De gebruikte perspectieven zijn:
Directie, ICT-Manager, Systeembeheerder, Infrastructuurbeheerder, Projectlid en Literatuur.

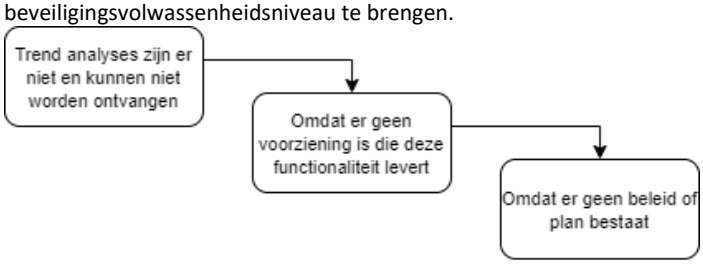
Perspectieven
Perspectieven worden opgehaald middels de uitgevoerde persoonlijke semigestructureerde interviews. De uitwerking van de perspectieven met de gerelateerde wensen en problemen worden hier uitgewerkt. Per perspectief wordt er een Root Cause Analyse uitgewerkt om zo onderliggende problemen juist uit te kunnen werken.

Perspectief van de directie:
In relatie tot deze casus/ het project wordt er aangegeven dat businesscontinuïteit het belangrijkste is en dat beveiliging hier nu aan bijdraagt. ICT staat steeds centraler in de organisatie en kort gezegd: “Het moet gewoon werken”. Hoewel kosten niet onbelangrijk zijn, mag het niet in de weg staan van een goede en gepaste oplossing. Kosten dienen overeenkomend tegenover de baten te staan. De directie ziet graag dat er meer focus komt op project en procesmatig werken, waarbij er rekening wordt gehouden met de complexiteit en integriteit van mogelijke aanbevelingen/ oplossingen. Momenteel is het proces en projectmatig werken (organisatie breed) nog niet het geval en zo heeft dit impact op de projecten en dagelijkse werkzaamheden.



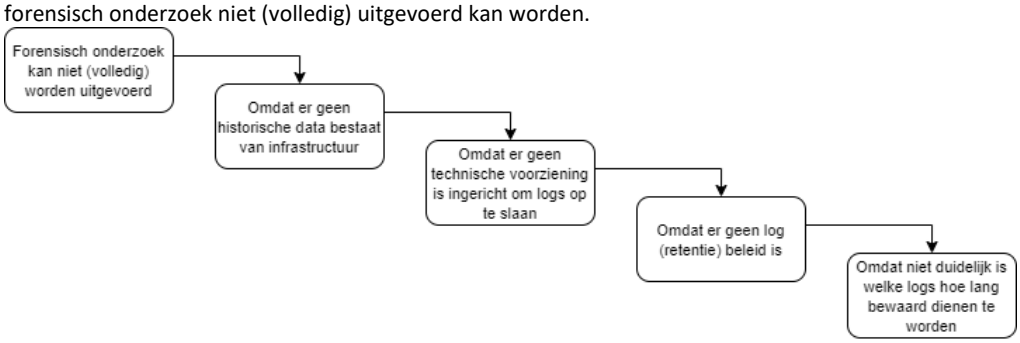
Figuur 5 Root Cause Analyse: Procesmatig werken

Perspectief van ICT-manager:
De ICT-manager geeft aan dat businesscontinuïteit voorop staat en dit altijd zo geweest is. In de hedendaagse wereld staat ICT echter zo centraal, dat beveiliging opeens een stuk belangrijker is. Beveiliging wordt nu steeds meer uitgevoerd om de continuïteit te waarborgen. De manager zou graag trendanalyses willen ontvangen, waarbij de focus ligt op preventieve en detectie (trend)analyses. Monitoring dient correct ingezet te worden om forensisch onderzoek uit te kunnen voeren. Processen mogen koste wat kost niet stil te komen liggen, beveiliging draagt daaraan bij. Vreemd gedrag herkennen is daar een belangrijk onderdeel van, maar dit gedrag hoeft überhaupt niet herkent te worden als het niet eens binnen kan komen. Preventie is daarom nog belangrijker dan detectie. Er wordt aangegeven dat de beveiliging van buitenaf dus het belangrijkste is. Er is bekend dat logging en events bij kunnen dragen aan de beveiliging, maar er is nog onduidelijk wat er nou exact gedaan kan worden met logs- en events. Het krijgen van een oplossing die ook daadwerkelijk doet wat een leverancier bijvoorbeeld biedt, zal wellicht de grootste succesfactor zijn. Daarbij is de grootste faalfactor wellicht wel dat een mogelijke oplossing niet doet wat een leverancier aangeeft dat het kan. De bedoeling van dit project is de organisatie op een hoger beveiligingsvolwassenheidsniveau te brengen.



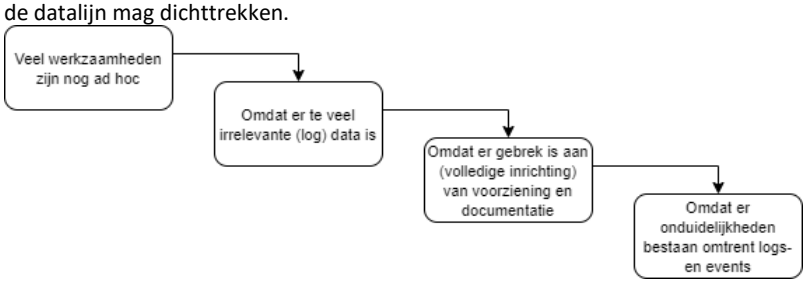
Figuur 6 Root Cause Analyse: Trendanalyses

Perspectief van Infrastructuurbeheerder:
Vanuit het perspectief van de Infrastructuurbeheerder wordt er aangegeven dat beveiliging, redundantie en een stabiele performance voorop staan. Er worden momenteel vooral meldingen en alerts ontvangen van onderdelen die gerelateerd zijn aan monitoring. De wens is om in de toekomst meer rapportages te krijgen, indien mogelijk op basis van trends. Monitoring moet worden ingezet om een stuk risicomanagement te kunnen uitvoeren, waarbij de verwachting is dat er in de toekomst ook meer naar governance gestuurd zal worden. De bedoeling is dan dat er meer processen en procedures uitgewerkt zullen worden, zodat er minder achter de feiten aan gelopen wordt. Op het moment dat er actie ondernomen moet worden, wordt dit op eigen initiatief en kennis gedaan. De infra-beheerder geeft aan zelf te weten wat en hoe er dingen moeten gebeuren. Een van de grootste problemen die Oosterberg nu ervaart is het niet kunnen inzien van historische data, waardoor een forensisch onderzoek niet (volledig) uitgevoerd kan worden.



Figuur 7 Root Cause Analyse: Forensisch onderzoek

Perspectief van Systeembeheerder:
De systeembeheerder geeft aan gebruik/ beheervriendelijke oplossingen en applicaties belangrijk te vinden. Iets moet bijvoorbeeld geautomatiseerd ingezet kunnen worden of met een paar klikken op de knop werken. Momenteel is er een operationeel beheerplan in ontwikkeling en bestaat er een minimaal ingezette Syslog-server, maar er wordt nog vrij weinig echt proactief gedaan. Oosterberg komt problemen tegen omdat er te veel irrelevante data is. Documentatie omtrent de inzichtelijkheid van potentiële datalekken of 'hoe te werken' op het moment dat zoiets voor komt bestaat nog niet. Een probleem dat uit het verleden impact heeft gehad op projecten is het feit dat er te weinig bandbreedte was bij Oosterberg tussen alle vestigingen. Er is inmiddels glasvezel aanwezig op alle vestigingen, maar dit betekent niet dat een oplossing alsnog de datalijn mag dichttrekken.



Figuur 8 Root Cause Analyse: Ad hoc werkzaamheden

Perspectief van de onderzoeker:
De onderzoeker heeft een onafhankelijke rol binnen dit project, waarbij er gekeken gaat worden naar de monitoringssituatie bij Oosterberg. Hierna worden er aanbevelingen en oplossingen uitgewerkt voor de problematiek die zich voordoet uit de organisatie. Vanuit dit onpartijdige perspectief zal het beste voor de betrokken partijen uit dit project worden gehaald.

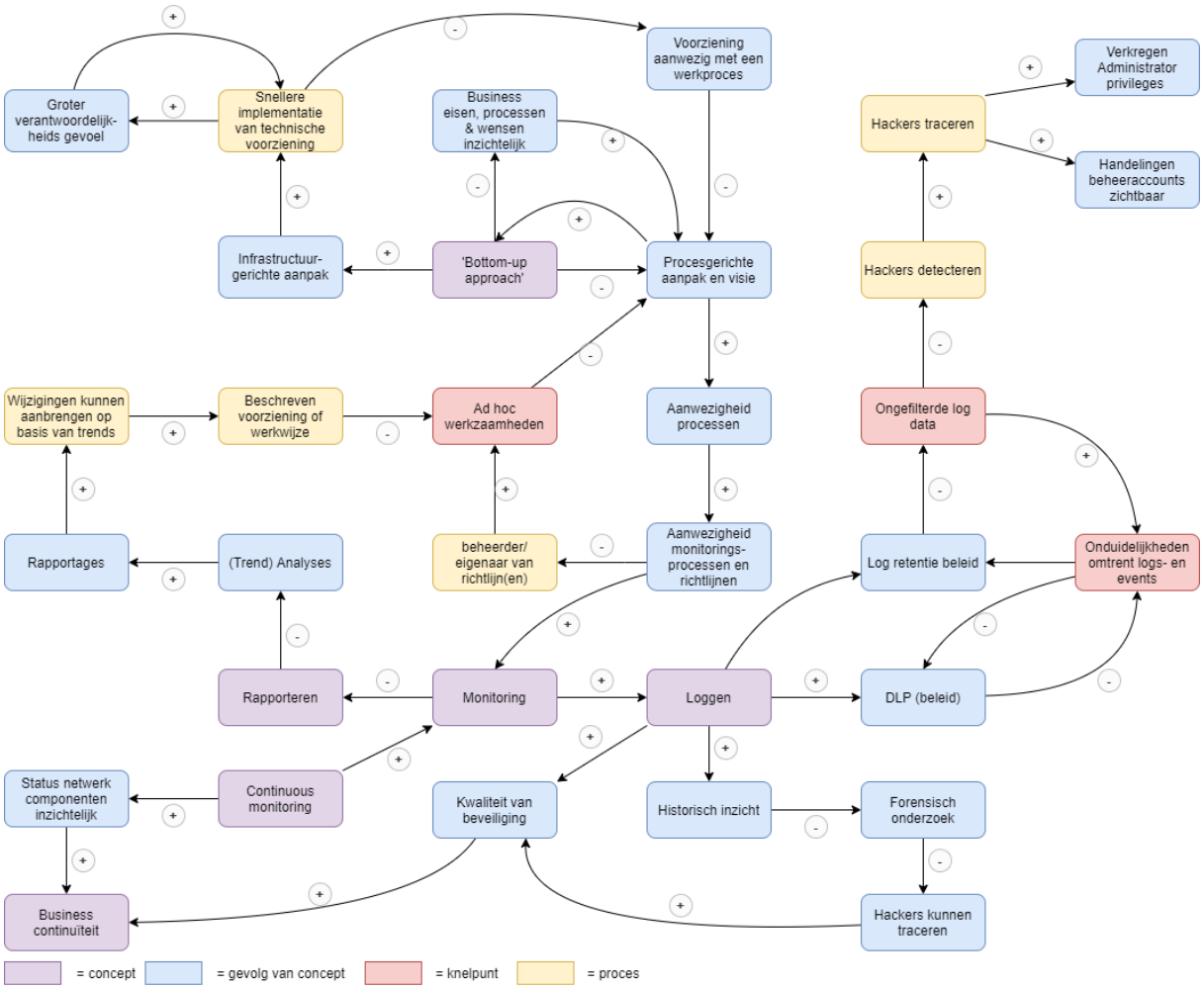
Perspectief van literatuur:
De bekeken literatuur laat zien dat monitoring een onderwerp is dat onderschat en met te veel gemak wordt opgepakt. Organisaties zien niet altijd wat de omvang is van monitoring en zetten dit vaak niet juist en/ of volledig in. Monitoring (goed inzetten) is een bekend 'probleem' of complex onderdeel van een IT-omgeving. Monitoring wordt vaak ingezet in de vorm van een technische oplossing, zonder hier op andere niveaus/ levels naar te kijken. Wanneer het eenmaal ingezet is, komt het ook vaak voor dat er te veel ongefilterde data opgehaald wordt (Boer, 2015). Technische oplossingen voor monitoring zijn bijvoorbeeld een (continuous)monitoringtool, een Syslog-server of een SIEM-oplossing. Overige belangrijke aspecten bij het inrichten van monitoring zijn architectuurprincipes en modellen, monitoringsprocessen, het volgen van top-down best practices, het opstellen van een log retentiebeleid en het eventueel inrichten en volgen van een monitoringsstandaard (SolarWinds MSP, 2020). Deze standaarden beschrijven, definiëren en geven richting aan het monitoren door bijvoorbeeld inzichtelijk te maken wat er gemonitord dient te worden. Hierbij wordt er onderscheid gemaakt tussen adviserende en eisende standaarden (Boer, 2015). Onderstaande standaarden worden vaak ingezet bij monitoring:

- COBIT, COSO, ISO 20000, 270001, 27002, ITIL, NIST 80053, SOX, HIPAA, FISMA en PCI DDS

Als monitoring op de juiste wijze wordt ingezet, kan het de businesscontinuïteit verhogen, beveiliging verder garanderen en kan het daarnaast zorgen voor zowel compliance, risicomanagement als governance (Boer, 2015).

Causaal relatiediagram
Om relaties inzichtelijk te maken tussen de verschillende eigenschappen (ofwel grootheden) wordt er een causaal relatiediagram ontworpen. De afhankelijkheden worden zo inzichtelijk gemaakt, waarbij te zien is dat het gaat om een dynamische omgeving. In dit diagram worden alle beschreven problemen en oorzaken vanuit de individuele perspectieven weergegeven. Ook onderdelen die benoemd of besproken zijn in de gesprekken tijdens de interviews worden hierin verwerkt. Op deze manier wordt er een compleet plaatje geschetst van de gehele organisatie met alle belangrijke aspecten.

In de tekening wordt onderscheid gemaakt tussen concepten, gevolgen, knelpunten en processen. Hierbij is te zien dat 'ad hoc werkzaamheden' een negatieve invloed hebben op procesgerichte aanpak en visie. Kortom, als deze werkzaamheden toenemen, dan neemt de procesgerichte aanpak af en als deze werkzaamheden afnemen, neemt de procesgerichte aanpak toe. Deze proceslijn is te volgen door de gehele tekening. Waarbij een procesgerichte aanpak ervoor zorgt dat processen aanwezig zijn, waardoor er processen en richtlijnen gevolgd kunnen worden, waardoor monitoring op juiste wijze ingericht kan worden. In de tekening zijn drie knelpunten te zien: Ad hoc werkzaamheden, ongefilterde log data en onduidelijkheden omtrent logs en events. Dit zijn de drie meest voorkomende constateringen vanuit de interviews. De bottom-up approach is niet geclassificeerd als een knelpunt omdat het ook voordelen met zich mee brengt.
Dit model laat zien wat de gevolgen zijn van deze knelpunten en hoe concepten opgesplitst worden.
De tekening kan 'gestart' worden bij het concept monitoren, dit concept wordt opgedeeld in drie andere concepten. Wanneer rapporteren wordt gevolgd, maakt rapporteren trend analyses mogelijk en zorgen deze analyses voor rapportages. Hierdoor kunnen wijzigingen worden aangebracht en kunnen voorzieningen of werkwijzen worden beschreven. Een toename aan beschrijvingen zorgt voor een afname aan ad hoc werkzaamheden. Een toename aan ad hoc werkzaamheden zorgt voor een afname aan procesgerichte aanpak. Een procesgerichte aanpak zorgt voor aanwezigheid van processen. Door deze processen en richtlijnen kan monitoren op juiste wijze worden ingericht. De overige concepten volgen dezelfde lijn met andere knelpunten, processen en gevolgen.



Figuur 9 Causale relatiediagram

4.2 Probleemstelling

De probleemstelling volgt uit de beschreven problematiek, die uitgewerkt zijn a.d.h.v. oorzaak-analyses. Dit komt tot stand door gebruik te maken van meerdere perspectieven.

Oosterberg ziet graag verbeteringen op gebied van cyber security, door het beter beheren van logs en het toepassen van monitoring en analyse. Forensisch onderzoek kan momenteel niet volledig uitgevoerd worden door een gebrek aan historische data, tijdige constateringen omtrent beveiligingslekken en het kunnen uitvoeren van analyses. Oosterberg zoekt naar een advies over hoe een monitoringoplossing ervoor kan zorgen dat bovenstaand genoemde onderdelen opgelost kunnen worden. Oosterberg wil graag adviezen over zo'n oplossing en op welke wijze dit het beste geïmplementeerd en geconfigureerd kan worden. Daarnaast wil Oosterberg graag weten hoe het beheerd dient te worden en hoe er procesmatig gehandeld kan worden op signaleringen vanuit het systeem. Oosterberg ziet graag aanbevelingen terugkomen uit het onderzoek, waarin geconcludeerd wordt waar de knelpunten in de huidige monitoringssituatie zitten. Er dient inzichtelijk gemaakt te worden waarom er bijvoorbeeld wel of niet een SIEM-oplossing ingezet kan worden, of het uitbesteed moet worden, wat er op korte en lange termijn behaald kan worden, of er alternatieven beschikbaar zijn naast de primaire aanbeveling(en) en waarom Oosterberg wel of niet zou kiezen voor bepaalde scenario's.

Doelstelling

- Koninklijke Oosterberg wil na afloop van het project advies hebben over hoe Oosterberg haar IT-omgeving weer onder controle kan krijgen door monitoring in te zetten. Oosterberg wil op een hoger beveiligingsvolwassenheidsniveau komen om businesscontinuïteit te garanderen, monitoring volgens best practices inrichten zal hieraan bijdragen.
- Oosterberg wil de betrouwbaarheid, integriteit en beschikbaarheid van de IT-systemen kunnen garanderen
- Oosterberg wil een technische oplossing kunnen inzetten om logs, events en rapportages te kunnen ontvangen en om forensisch onderzoek uit te kunnen voeren

Hoofdvraag

Hoofd- en deelvragen worden afgeleid uit de bovenstaande probleemstelling. Hierbij wordt de onderstaande hoofdvraag geformuleerd:

- *"Hoe kan Koninklijke Oosterberg B.V. het monitoren optimaal en centraal inrichten?"*

Deelvragen

Het beantwoorden van de hoofdvraag wordt gedaan a.d.h.v. deelvragen. Onderstaande deelvragen geven uiteindelijk antwoord op de hoofdvraag:

- Wat zijn de knelpunten in de huidige situatie?
- Wat is de architectuur van de huidige situatie?
- Wat zijn de eisen die Oosterberg stelt?
- Welke mogelijke conceptuele oplossingen zijn er?
- Wat is de impact van een oplossing op de bestaande omgeving?
- Wat is de architectuur van de toekomstige situatie?

5 Vooronderzoek

In het vooronderzoek worden een tweetal analyses uitgevoerd. Analyses zullen parallel met elkaar worden uitgevoerd. Het vooronderzoek mondt uit in de eisen, wensen en randvoorwaarden van de opdracht met daarbij een duidelijk probleem. Na het vooronderzoek kan de literatuurstudie gestart worden. De onderdelen die worden behandeld in het vooronderzoek zijn:

- Behoefteanalyse, resulterend in geprioriteerde eisen en wensen;
- Contextanalyse, resulterend in de huidige situatie en randvoorwaarden.

5.1 Behoefteanalyse

Inleiding

Een behoefteanalyse zal resulteren in een eisen en wensen (requirements) lijst. Deze lijst van eisen en wensen wordt geprioriteerd door het toepassen van de MoSCoW-methodiek. De requirements zullen daarnaast ook SMART-geformuleerd* zijn. Voordat er genoteerd wordt wat de daadwerkelijke eisen en wensen zijn, is het van belang dat duidelijk is waar deze informatie vandaan is gehaald. Om dit aan te geven wordt er in de onderstaande kop aangeduid welke bronnen, welke perspectieven en welke data er gebruikt is om tot deze eisen te komen. I.v.m. de grootte van de scriptie en de leesbaarheid van het document wordt hieronder alleen de shortlist met de requirements-lijst opgenoemd. De longlist met de analyse en bepaling van stakeholders staat in de behoefteanalyse bijlage.

**Specifiek, Meetbaar, Acceptabel, Realistisch, Tijdsgebonden.*

Shortlist

Na het uitwerken van een longlist kan er een shortlist opgesteld worden. Deze shortlist beschrijft de belanghebbenden met de meeste macht en interesse binnen dit project. Aan de perspectieven vanuit deze belanghebbenden zal de meeste aandacht worden besteed. Onderstaande shortlist wordt gebruikt:

- Directie
- ICT-Manager
- Systeembeheerder
- Infrastructuurbeheerder

Requirements

Alle requirements worden genoteerd en opgesteld in een tabel. Indicaties worden opgedeeld in 3 categorieën:

- **Business**: Een eis vanuit de organisatie. (B)
- **User**: Een eis vanuit de gebruiker. (U)
- **Systeem**: Een technische eis. (S)

Prioriteiten worden aangegeven d.m.v. de MoSCoW-methodiek.

- **Must**: Deze eis is essentieel voor het project en dient absoluut behaald te worden.
- **Should**: Deze eis is gewenst en dient indien mogelijk zeker meegenomen te worden.
- **Could**: Deze eis kan als optioneel/ extra worden beschouwd en dient alleen meegenomen te worden indien budget en tijd dit toestaan.
- **Won't have (now)**: Dit hoort tot nazorg of opvolgingsfase van het project en wordt nu niet opgepakt.

De verkregen informatie komt uit de interviews met de vier belangrijkste stakeholders uit de geformuleerde shortlist. Functionele en niet functionele eisen worden aan de rechterkant van de tabel gecategoriseerd. (F/ NF)

Alle eisen dienen behaald te worden voor 13-06-2021 en zijn daarom tijdsgebonden. Dit wordt bovenaan de tabel aangegeven om leesbaarheid van de tabel te waarborgen.

ID	Correlatie	Requirement	Stakeholder	F/ NF
		Must have requirements		
REQ-B-01		De kosten van een oplossing dienen goed overeen te komen met de baten, maar kosten zijn geen showstopper	ICT-Directeur	NF
REQ-B-02		Er dienen (trend)rapportages opgehaald te kunnen worden, dit betreft rapportages zoals het inzien van toename aan data in gebruiker mail, profiel en OneDrive	ICT-Directeur	NF
REQ-B-03		Er dienen analyses uitgevoerd te kunnen worden op basis van trends en afwijkingen in deze trends, dit betreft trends zoals het inzien van toename aan data in gebruiker mail, profiel en OneDrive	ICT-Manager	NF
REQ-B-04		Vervolgstappen a.d.h.v. dit project dienen inzichtelijk gemaakt te worden	ICT-Directeur	NF
REQ-B-05		Gebruikersondersteuning dient snel aangevraagd te kunnen worden, waarbij de organisatie geholpen wordt door een partner door support en wellicht bij implementatie en/ of beheer	ICT-Manager	NF
REQ-B-06		Bedrijfscontinuïteit dient bewaakt te worden door de verhoging van het beveiligingsniveau, waarbij op lange termijn het tactische niveau behaald dient te worden en op korte termijn het proactieve (volwassenheid)niveau	Infra-beheerder	NF
REQ-B-07		Het inrichten van mogelijke KPI's voor ICT dient bestudeert te worden	ICT-Directeur	NF
REQ-U-01		Log data dient compacter, meer gecentraliseerd en informatiever gemaakt te worden	Systeembeheerder	NF
REQ-U-02		De oplossing dient gebruik- en beheers vriendelijk te zijn, het mag niet te complex worden en dient daarom intuïtief te werken en/ of in te spelen op bestaande werkzaamheden. Dit zal moeten blijken uit mogelijke reviews van een oplossing	Systeembeheerder	NF
REQ-U-03	REQ-B-03 REQ-B-04	Er dient duidelijk te worden gemaakt welke logs hoelang en waar bewaard moeten worden	ICT-Manager	NF
REQ-U-04		Er dient inzichtelijk te worden gemaakt wat best practices omtrent monitoring zijn	ICT-Manager	NF
REQ-U-05		De oplossing dient een voorziening te hebben om te kunnen filteren en zoeken	ICT-Manager	F
REQ-U-06	REQ-B-03 REQ-B-04	De oplossing dient eventherkenning te hebben om te zien welke events wanneer voor komen	ICT-Manager	F
REQ-U-07	REQ-B-03 REQ-B-04	De oplossing dient zowel on premise als in de Cloud (Azure) logs op te kunnen halen	ICT-Manager	F
REQ-U-08		De oplossing dient een ingebouwd managementsysteem te hebben om meldingen goed te kunnen keuren	ICT-Manager	F
REQ-U-09		Historische data dient beschikbaar te worden gemaakt voor forensisch onderzoek	Infra-beheerder	F
REQ-S-01	REQ-B-01 REQ-B-07	De oplossing dient voor zover mogelijk gescheden te zijn van de bestaande infrastructuur i.v.m. veiligheid en beschikbaarheid	ICT-Manager	F
REQ-S-02	REQ-B-03 REQ-B-04	De oplossing dient te integreren te zijn met de huidige infrastructuur en omgeving	Infra-beheerder	F
REQ-S-03	REQ-B-01	Er dient aangetoond te worden wat de impact op systeemperformance is van een oplossing. Een oplossing mag de systemen niet traag maken	Infra-beheerder	F
		Should have requirements		
REQ-U-10		De oplossing moet aantonen dat er een hacker is en welke rechten deze hacker heeft verkregen	ICT-Manager	F
REQ-U-11		De oplossing dient 'severity scores' te kunnen hangen aan events die meer prioriteit verdienen om zaken te kunnen managen en overzichtelijk te houden	ICT-Manager	F
REQ-S-04	REQ-U-02	De oplossing moet kunnen automatiseren d.m.v. het gebruik van templates	Systeembeheerder	F
REQ-S-05	REQ-U-02	De oplossing dient systeemherkenning te hebben op basis van type of merk. De oplossing dient veel intelligentie met de oplossing mee te komen, waardoor beheer en inrichting eenvoudig worden gemaakt	ICT-Manager	F
REQ-S-06	REQ-U-06	Oosterberg wil graag weten of het mogelijk is om meer applicaties te loggen of te integreren. Integratiemogelijkheden omtrent o365 zijn van belang	ICT-Manager	F
		Could have requirements		
REQ-S-07	REQ-U-06 REQ-U-07	De oplossing dient geïntegreerd te kunnen worden met TopDesk of dient zelf 'tickets' te managen	ICT-Manager	F
		Won't have now		
REQ-B-08	REQ-B-08	Het inrichten van KPI's dient voor ICT gerealiseerd te worden	ICT-Directeur	NF
REQ-B-09	REQ-U-03	Het opstellen van een logretentiebeleid dient gerealiseerd te worden	Infra-beheerder	NF
REQ-U-12	REQ-U-06 REQ-U-07	Het inrichten van een documentatie managementsysteem dient gerealiseerd te worden	Systeembeheerder	F

Tabel 4 Conclusie behoefteanalyse: Requirements

5.2 Contextanalyse

De contextanalyse geeft een inzicht in de huidige situatie van Oosterberg. De (organisatie)context wordt bekeken en hier worden randvoorwaarden uitgehaald. Deze analyse wordt uitgevoerd door gebruik te maken van verschillende aggregatieniveaus en aspecten. Deze informatie wordt gehaald uit interviews en deskresearch.
De informatie wordt verwerkt door een verander kaleidoscope (model) uit te werken. De huidige situatie wordt in kaart gebracht door ArchiMate toe te passen op basis van de TOGAF-methode.
Onderstaande stappen worden uitgevoerd om uiteindelijk te kunnen concluderen in de randvoorwaarden:

- Onderzoeken van te gebruiken aggregatieniveau(s) en aspecten
- Uitvoeren van interviews met stakeholders om randvoorwaarden vast te stellen
- Uitwerken van de randvoorwaarden en de contextanalyse daarmee concluderen

Aggregatieniveaus
Door het uit voeren van deskresearch kan het vaststellen van de niveaus op onderstaande wijze worden gedaan:
Micro**:**
Onder het aggregatieniveau Micro wordt er gekozen voor Oosterberg. Dit abstractieniveau duikt in op de organisatiecontext. Door hiervoor te kiezen kan er worden gekeken naar alle aspecten van de organisatie en wordt niets achterwege gelaten.
Meso**:**
Onder het aggregatieniveau Meso wordt er gekozen voor de directe bedrijfsomgeving. Op deze manier wordt de methode 'micro, meso en macro' gehandhaafd. Dit zorgt er echter ook voor dat dit onderdeel niet wordt toegelicht, omdat het buiten de projectscope valt.
Macro**:**
Onder het aggregatieniveau Macro wordt er gekozen voor maatschappelijke krachten. Het wordt aangeraden om minimaal één niveau boven het werkniveau mee te nemen (Haveman, Hageraats, & Linden, 2016). Op deze manier worden er aan de weerszijden van de Meso- omgeving verschillende niveaus bekeken. Ook dit niveau wordt verder niet toegelicht omdat het buiten de projectscope valt. De maatschappelijke invloeden zoals politieke of demografische veranderingen hebben geen invloed hebben op dit project. Rechter afbeelding visualiseert dit:

Figuur 10 Aggregatieniveaus

Aspecten
Op basis van de aggregatieniveaus worden aspecten bepaald. Door deskresearch toe te passen, persoonlijke interviews te houden en groepsgesprekken uit te voeren, kunnen de aspecten worden gedefinieerd. De bepaling van relevantie interviewvragen staat in de interviewvragen-bijlage.
Onderstaand de opsomming van aspecten:

- Beveiligingsaspect
  - Dit aspect staat centraal in dit project en kijkt op de diverse niveaus naar randvoorwaarden op het aspect 'beveiliging'. Beveiliging is een behoefte die belangrijk is voor alle belanghebbenden.
- Beheeraspect
  - Het beheren van diverse oplossingen en de wijze waarop dit wordt gedaan is wellicht het allerbelangrijkste voor dit project, helemaal wanneer hier mogelijke veranderingen plaatsvinden. Mogelijke beperkingen worden in kaart gebracht door dit aspect onder de loep te nemen. Beheer zal bijdragen aan het behalen van het doel en een betere beveiliging.
- Financieel aspect
  - Uit interviews blijkt dat kosten geen showstopper zullen zijn, maar er wordt aangegeven dat er wel een duidelijke en goede overeenkomst moet zijn tussen de kosten en baten. Het financiële aspect duikt kort in op de mogelijke kosten en de relatie van deze kosten aan dit project.
- Tijdsaspect
  - Tijd is bij elk project van belang, omdat het beperken van tijd ervoor zorgt dat het project op lange en korte termijnen doelen kan stellen.
- Technisch aspect
  - Het technische aspect duikt in op de niveaus om te kijken of er technische beperkingen bestaan waar tijdens dit project rekening mee gehouden dienen te worden. Omdat het een IT-gerelateerd project is, is de kern van dit project technisch ingericht.

Vaststellen van randvoorwaarden per aggregatieniveau
In dit onderdeel worden de randvoorwaarden vanuit de micro-omgeving per aspect ingedeeld en beschreven. I.v.m. relevantie aan het project worden de meso en macro-omgeving buiten beschouwing gelaten. Het verkrijgen van deze randvoorwaarden wordt gedaan d.m.v. deskresearch en het uitvoeren van persoonlijke semi/ half gestructureerde interviews.

Micro – Oosterberg
Beveiligingsaspect

- De oplossing dient bij te dragen aan het verhogen van de businesscontinuïteit

- In de context van monitoringstandaarden dient het onderzoek een focus te hebben op ISO-monitoringstandaarden
- Het onderzoek dient overige monitoringstandaarden buitenwege te laten

Beheeraspect

- De huidige bezetting op de ICT-afdeling met al haar competenties dient om te kunnen gaan met een oplossing
- De oplossing dient ondersteund te kunnen worden door een goede kennisvolle partner waarmee samengewerkt kan worden. Een willekeurig van het internet afgeplukte tool is een no-go
- De oplossing dient bij te dragen aan procesgericht werken
- De oplossing dient bij te dragen aan projectgericht werken
- De oplossing mag geen nadelige werking hebben op de bestaande processen

Financieel aspect

- De aanschaf van hard- en software van een mogelijke oplossing valt niet binnen dit project
- Kosten en baten dienen een goede verhouding te hebben

Tijdsaspect

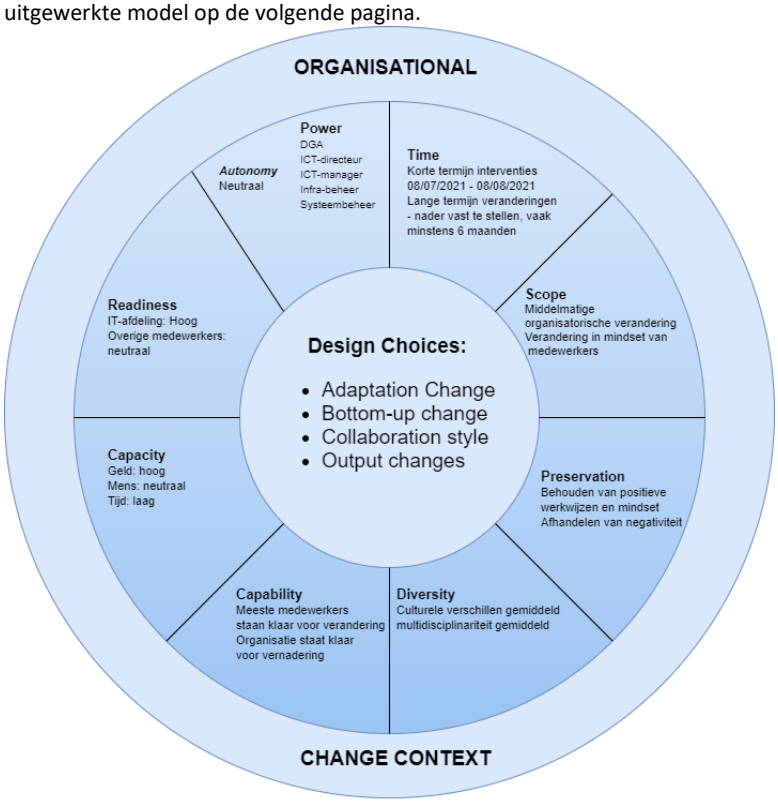
- Er dient onderzocht en ontworpen te worden, implementatie valt buiten deze tijdsomvatting

Technisch aspect

- De oplossing zal moeten werken op de bestaande infrastructuur, het moet niet zo zijn dat deze infrastructuur aangepast moet worden om met de oplossing overweg te kunnen
- De oplossing mag geen nadelige werking hebben op de performance van de infrastructuur en daarbij horende applicaties
- Het project richt zich en beperkt zich tot de on premise omgeving van Oosterberg met de daarbij horende Azure omgeving van Oosterberg en houdt zo rekening met de hybride opzet
- Op het moment dat er een geschikte oplossing gevonden is, dient er ook een partij te zijn die helpt met de implementatie, beheer en support van deze oplossing

<u>Organisatie contextanalyse</u>

Het in kaart brengen van de organisatie en haar context is een belangrijk onderdeel van de contextanalyse. Omdat de Micro-omgeving 'Oosterberg' omvat, wordt deze analyse hier uitgevoerd. De organisatie contextanalyse wordt uitgevoerd door een (verander) kaleidoscope te gebruiken. Dit model hanteert verschillende dimensies die inzicht bieden in de organisatie en haar context. De verander kaleidoscope wordt ook toegepast om sterke en zwakke punten weer te geven van toekomstige interne veranderingen. Aspecten zoals belanghebbenden, tijd en geld worden weergegeven om een zo'n breed mogelijk beeld te vormen van de organisatie en de mogelijke veranderingen. De informatie kan per dimensie worden ingedeeld door gebruik te maken van de informatie die opgehaald is uit deskresearch en de uitgevoerde interviews. Per onderdeel zal een aparte toelichting plaatsvinden om verwarring te voorkomen en duidelijkheid te waarborgen. Toelichtingen van de middelste en binnenste cirkels kunnen worden gevonden in de contextanalyse bijlage. Zie het uitgewerkte model op de volgende pagina.



Figuur 11 Verander Kaleidoscope (DOEN, 2021)

Toelichtingen:
Bij dit onderdeel worden de toelichtingen over de aspecten van de verander kaleidoscope beschreven. Er zal van buiten naar binnen worden gewerkt, waarbij eerste de buitenste (organisatie context) ring wordt beschreven.
De kaleidoscope heeft drie ringen:

- De buitenste ring heeft betrekking op de bredere strategische context.
- De middelste ring heeft betrekking op specifieke contextuele factoren waarmee rekening moet worden gehouden bij het doorvoeren van eventuele veranderingen.
- De binnenste cirkel geeft een menu met keuzes en interventies ('ontwerpkeuzes') die beschikbaar zijn om de betreffende onderdelen te kunnen veranderen. Deze interventies zullen kort beschreven worden maar dit zal uiteindelijk buiten de scope van dit project vallen.

Buitenste cirkel – Organisatie context:

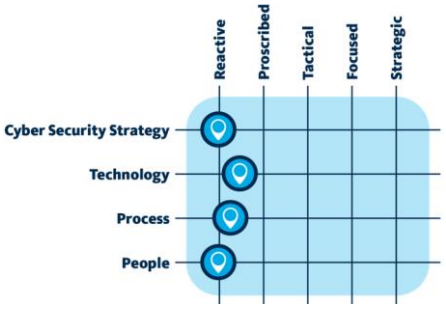
Koninklijke Oosterberg B.V. is een elektrotechnische groothandel en zit zo ook in de sector detailhandel/ elektrotechnische groothandel. Het is een familiebedrijf en groeit én stuurt met de markt mee. Uit oorsprong was het bedrijf begonnen als pianobouwer en nu is het bedrijf terecht gekomen in de elektrotechnische groothandel. De hoofdlocatie van het bedrijf is gevestigd in Apeldoorn, vlak naast het distributiecentrum. Het bedrijf heeft inmiddels 21 vestigingen verspreid over heel Nederland.
Oosterberg heeft een marktaandeel van rond de 10/ 15% en heeft 23940 klanten, waarvan er 13080 echt actief zijn, daarmee is Oosterberg de 3e grootste elektro-groothandel in Nederland. Daarbij heeft het bedrijf 400 medewerkers, waarvan er zo'n 250 op het kantoor werken met bijbehorende Office-licenties.
De ICT-afdeling kan worden opgedeeld in zo'n 8 tot 10 medewerkers (i.v.m. openstaande vacatures en inhuurkrachten), waarbij er onderscheid wordt gemaakt tussen applicatiebeheer en systeembeheer.
Onderling wordt daar verder nog onderscheid gemaakt tussen infrastructuurbeheer, database en projectbeheer.

Oosterberg neemt net het extra stapje en steekt als het ware de nek uit voor haar klanten. Het levert meer dan alleen een oplossing en probeert zo goed mogelijk, op maat gemaakte oplossingen voor klanten te bieden met een uitstekende service. Als de markt zich ergens naartoe beweegt, dan weet Oosterberg als geen ander hierin mee te gaan. In het bedrijf heerst een informele sfeer, waarbij er op een samenwerkende manier leiding wordt gegeven. Hoewel er een zekere scheiding in niveaus en functies aanwezig moet zijn i.v.m. de grootte van de organisatie, is het doel om de organisatie zo 'plat mogelijk' in te delen.
Oosterberg merkt dat ICT steeds centraler komt te staan in de organisatie. Voorheen kon het worden gezien als hulpmiddel, maar ondertussen houdt het de organisatie draaiende. Business continuïteit staat net als vroeger nog steeds voorop, maar beveiliging wordt ook steeds belangrijker. Beveiliging zal nu ingezet moeten worden om een stuk risicomanagement te kunnen uitvoeren, zodat de businesscontinuïteit gewaarborgd kan worden en het bedrijf op een hoger beveiligingsvolwassenheidsniveau terecht komt.
Een van de grote interne projecten is het inrichten van de juiste monitoringsoplossing/ omgeving, waarbij de onderstaande problematische punten aangepakt dienen te worden:

- Forensisch onderzoek kan niet volledig worden uitgevoerd door gebrek aan logs
- Beschikbare gelimiteerde log data bestaat in te grote bulk
- Analyses en op basis van trends met daaruit voortvloeiende rapportages zijn er niet

Deze problematiek kan aangepakt worden door dit onderzoekstraject/ project, waarbij er gekeken wordt naar een nieuwe monitoringsoplossing voor Oosterberg. Deze oplossing komt terecht op de ICT-afdeling (automatiseringsafdeling).

Huidige situatie
Voordat de contextanalyse wordt afgerond met de randvoorwaarden, wordt de huidige situatie bekeken. De informatie om dit tot stand te laten komen is verkregen door deskresearch en interviews uit te voeren.
Oosterberg wil naar een hoger beveiligings- volwassenheidsniveau, omdat ICT momenteel op het 'reactieve' niveau zit en naar het 'tactische' niveau wil. Bij het uitgevoerde security assessment door Fox-IT (Bresser, 2020) is er gekeken naar meerdere variabelen, deze zijn te zien in rechter tabel. Er wordt zo onderscheid gemaakt tussen: Cyber Security Strategie, Technologie, Proces en Mens.



Figuur 12 Huidig opgedeeld securityniveau (Bresser, 2020)

Uit dit assessment worden de volgende toelichtingen bij de verschillende onderdelen beschreven:
Kijkend naar de huidige kwetsbaarheden en getroffen maatregelen wordt het huidige volwassenheidsniveau van Oosterberg geclassificeerd als **Reactief** (Reactive) op alle aspecten. Dit wordt onderscheiden op basis van de volgende observaties:

- **Cyber Security Strategie:** De strategie is beperkt sturend geformuleerd en in de praktijk wordt weinig concrete invulling gegeven aan een strategie.
- **Technology:** Oosterberg beschikt over enkele goede technische mogelijkheden. Deze worden echter beperkt effectief ingezet. Daarnaast ontbreekt het aan technische maatregelen die bescherming moeten bieden aan de meeste dreigingen.

- **Proces:** Processen rondom cyber security ontbreken of worden niet consistent gevolgd.
- **People:** Er is onvoldoende aandacht voor Security Awareness (Bresser, 2020).

Uit bovenstaande informatie kan geconcludeerd worden dat er meerdere onderdelen zijn die verbeterd moeten worden. Monitoring is een van de onderdelen die essentieel is om ervoor te zorgen dat de niveaus op een hoger level terecht komen. Hierbij is het de bedoeling dat er vanuit een reactieve situatie op korte termijn naar een proscribed situatie kan worden gewerkt en op lange termijn is het vervolgens de bedoeling dat het tactische niveau behaald wordt.
Uit de interviews kan geconstateerd worden dat Oosterberg een focus heeft op businesscontinuïteit en ook daarvoor de beveiliging inzet. Het gaat niet zozeer om het verliezen van data, maar meer om het draaiend houden van de logistieke processen. Dit mag niet stil komen te liggen door onder andere ransomware en andere gijzel of hackpogingen.
De 'waaromvraag' bij Oosterberg wordt beantwoord door diezelfde interviews. Uit deze interviews kan gesteld worden dat Oosterberg monitoring in wil zetten om een stuk risicomanagement op te pakken en te garanderen.
Risicomanagement is het primaire doel i.v.m. het willen beschermen tegen dreigingen, forensisch onderzoek willen uitvoeren en het willen bewaken van de integriteit en beschikbaarheid (businesscontinuïteit) van de infrastructuur. Het organisatiebelang bij deze opdracht luidt daarom als volgt:
'Oosterberg wil de betrouwbaarheid, integriteit en beschikbaarheid van de IT-systemen en infrastructuur kunnen garanderen, omdat businesscontinuïteit voorop staat'.
Het is belangrijk om te noteren dat er vanuit Oosterberg wel aan wordt gegeven dat de organisatie in de toekomst ook steeds meer naar een stukje (IT) governance wil, dit blijkt uit interviews met ICT-Directeur en infrastructuurbeheerder. De onderbouwing hiervoor is dat er op termijn meer IT-performance management uitgevoerd zal gaan worden. Asset, configuration, incidentmanagement en ook riskmanagement zijn hier voorbeelden van. Hoewel dit gedeeltelijk buiten de projectscope valt, zijn het wel onderdelen die meegenomen kunnen worden in onderbouwingen, aanbevelingen en in de nazorg van het project.
Tot slot zijn subonderdelen van het concept 'monitoring' al opgepakt bij Oosterberg. PRTG (monitoring) wordt uitgebreider ingezet, het actief monitoren van actuele data wordt zo al een stuk beter en breder opgepakt. Tevens is er een Syslog-oplossing op gelimiteerde wijze geïmplementeerd op het netwerk. Tot slot is ook het continu scannen naar kwetsbaarheden (CVE's) opgepakt door het inzetten van de oplossing Holm Security.

Voor een uitgebreide analyse van de huidige logging-situatie en het monitoringvolwassenheidsniveau, zie de contextanalyse bijlage.

Architectuur van de huidige situatie
In dit onderdeel wordt de architectuur van de huidige situatie bekeken. Dit kan worden gedaan door de bevindingen uit de interviews te gebruiken, deskresearch uit te voeren en deze vervolgens uit te werken door de tool ArchiMate a.d.h.v. de methodiek TOGAF.
Het inzetten van het concept 'monitoring' is een van de onderdelen die de organisatie op een hoger beveiligingsniveau zal krijgen, maar het zal niet zomaar voldaan zijn. Om op juiste wijze naar een hoger volwassenheidsniveau te komen, zullen een aantal onderdelen aangepakt moeten worden. Onderstaande punten zijn een globale opsomming van deze onderdelen:

- ICT-beleid, ICT-beleidsplan
- Architectuurprincipes
- Architectuurmodellen (Boer, 2015)

Hierbij is het van belang dat er genoteerd wordt dat er geen officieel ICT-beleid is, waardoor het niet mogelijk is om architectuurprincipes te kunnen ontwerpen. Oosterberg wil de betrouwbaarheid, integriteit en beschikbaarheid van de IT-systemen en infrastructuur kunnen garanderen, omdat businesscontinuïteit voorop staat. Om de problemen concreet in kaart te kunnen brengen, zal de huidige overkoepelende situatie bekeken moeten worden. Het in kaart brengen van deze situatie wordt gedaan door de IST-situatie uit te werken. De IST-situatie is de huidige situatie.
Het ontwerpen van deze architectuurmodellen wordt gedaan door onderscheid te maken in een drietal lagen:

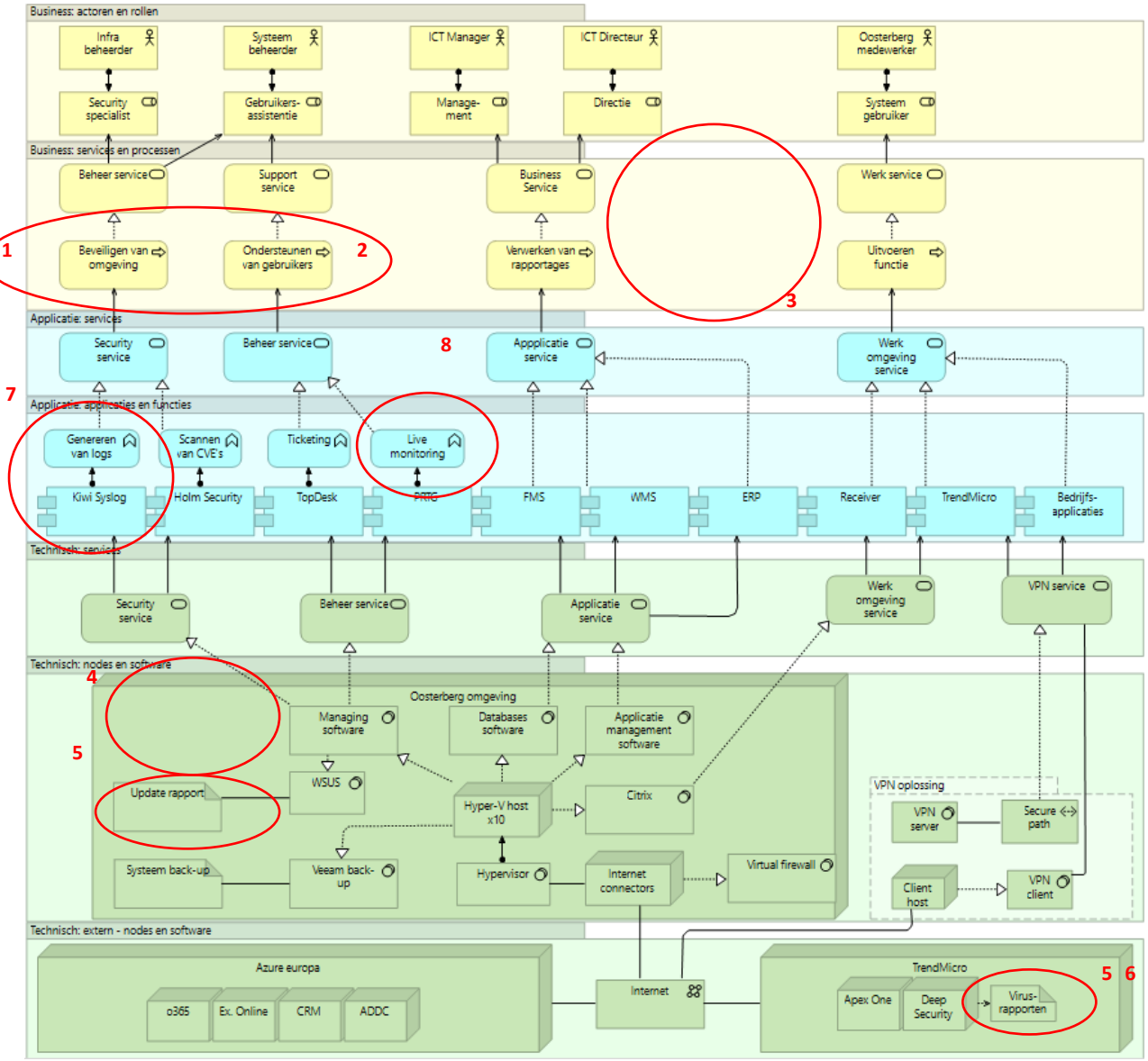
- Business;
- Applicatie;
- Systeem

Toelichting architectuurindeling:
Alle toelichtingen zijn algemene beschrijvingen van er normaliter te vinden is op de lagen, dit kan betekenen dat niet alle onderdelen altijd aanwezig zijn. Als een onderdeel niet aanwezig is, wordt dit omcirkelt en beschreven in de bevindingen en conclusies. Dit wordt gedaan om leesbaarheid te waarborgen en te garanderen dat de architectuurtekening valide wordt opgebouwd.

- De business laag staat aangegeven d.m.v. de gele kleur. De business-laag geeft weer welke actoren er zijn, wat voor rollen deze personen (actoren) hebben en welke processen deze personen uitvoeren.
- De applicatie laag wordt weergegeven door de blauwe kleur en geeft weer welke applicaties, functies en services er allemaal zijn in de omgeving.
- De technisch laag zal worden aangegeven door de groene kleur en zal aangeven hoe de infrastructuur van Oosterberg eruitziet. Dit is een globale weergave van de bestaande koppelingen.

Zie ontworpen architectuur en de daarbij horende toelichting op de volgende pagina.

Architectuurontwerp



Figuur 13 Architectuur van de huidige situatie

Constateringen en bevindingen

Onderstaande opsomming beschrijft de belangrijkste aspecten uit dit architectuurontwerp en zijn terug te vinden in de architectuurtekening door de rode cirkels. Deze informatie komt voort uit de uitgevoerde interviews met alle belanghebbenden en door deskresearch uit te voeren.

1. Er bestaan geen beschreven (monitoring)processen.
2. Het is voor de medewerkers duidelijk wat de werkzaamheden zijn, alleen staan deze niet tekstueel beschreven. Deze werkzaamheden zijn daarnaast niet gebaseerd op documenten of regels.
3. Actoren willen meerdere (trend)rapportages krijgen, maar ontvangen deze nu niet.
4. Er kunnen geen (trend)analyses worden uitgevoerd op de infrastructuur door gebrek aan inrichting van technische voorziening of aanwezigheid van deze voorziening en het gebrek aan procesmatige inrichting.
5. Rapportages komen alleen voort uit Trend Micro antivirus en WSUS, overige rapportages zijn er niet.
6. Systeem en Infra-beheerders krijgen updates op de automatiseringsmail vanuit onder andere Trend Micro virusmeldingen, quarantaine meldingen en foutieve loginpogingen vanuit de Syslog server.
7. Syslog is kleinschalig ingericht, alleen data van de managementserver en data van coreswitches staat hier nu in.
8. PRTG maakt actuele status van machines duidelijk en verstuurd meldingen in de vorm van e-mails, maar er is geen centraal overzichtsbord ingericht.

Conclusie contextanalyse

Door het toepassen van de verschillende methodieken (interviews, analyses, deskresearch) worden de context van de organisatie en de projectrandvoorwaarden in kaart gebracht. In onderdeel "*Vaststellen van randvoorwaarden per aggregatieniveau*" zijn de randvoorwaarden per aspect ingedeeld, maar zal op overzichtelijke wijze hier in tabelweergave geconcludeerd worden wat de randvoorwaarden van dit project zijn.

ID	Randvoorwaarde	Aspect
RV-01	De oplossing dient bij te dragen aan het verhogen van de businesscontinuïteit	Beveiliging
RV-02	In de context van monitoringstandaarden dient het onderzoek een focus te hebben op ISO-monitoringstandaarden	Beveiliging
RV-03	Het onderzoek dient overige monitoringstandaarden buitenwege te laten	Beveiliging
RV-04	De oplossing dient bij te dragen aan procesgericht werken	Beheer
RV-05	De oplossing dient bij te dragen aan projectgericht werken	Beheer
RV-06	De huidige bezetting op de ICT-afdeling met al haar competenties dient om te kunnen gaan met een oplossing	Beheer
RV-07	De oplossing dient ondersteund te kunnen worden door een goede kennisvolle partner waarmee samengewerkt kan worden. Een willekeurig van het internet afgeplukte tool is een no-go.	Beheer
RV-08	De oplossing mag geen nadelige werking hebben op de bestaande processen	Beheer
RV-09	De aanschaf van hard- en software van een mogelijke oplossing valt niet binnen dit project	Financieel
RV-10	Kosten en baten dienen een goede verhouding te hebben	Financieel
RV-11	Er dient onderzocht en ontworpen te worden, implementatie valt buiten deze tijdsomvatting.	Tijd
RV-12	De oplossing zal moeten werken op de bestaande infrastructuur, het moet niet zo zijn dat deze infrastructuur aangepast moet worden om met de oplossing overweg te kunnen	Technisch
RV-13	De oplossing mag geen nadelige werking hebben op de performance van de infrastructuur en daarbij horende applicaties	Technisch
RV-14	Het project richt zich en beperkt zich tot de on premise omgeving van Oosterberg met de daarbij horende Azure omgeving van Oosterberg en houdt zo rekening met de hybride opzet	Technisch
RV-15	Op het moment dat er een geschikte oplossing gevonden is, dient er ook een partij te zijn die helpt met de implementatie van deze oplossing	Technisch

Tabel 5 Randvoorwaarden

6 Literatuuronderzoek

Het literatuuronderzoek zal antwoord geven op de deelvraag 'wat zijn mogelijke conceptuele oplossingen?'. Deze deelvraag wordt gebruikt om vervolgens de hoofdvraag te kunnen beantwoorden. Dit is een onderzoekend project, waarbij het literatuuronderzoek niet de enige fase is waarbij er wordt onderzocht. Veel informatie, kennis, conclusies en bevindingen zijn al geformuleerd bij het vooronderzoek. Bij het uitvoeren van het literatuuronderzoek dienen een aantal onderwerpthema's het onderzoek te omvatten. Onderstaande thema's omvatten het onderzoek en worden door te brainstormen verkregen:
Best Practices, Monitoring, Standaarden, Strategieën, Protocollen, Loggen, Technische oplossing, Rapporteren.

Onderstaande stappen worden uitgevoerd om het literatuuronderzoek juist uit te voeren:

- Beschrijven van gebruikte methodieken
- Elke deelvraag dient een literatuuronderzoek te krijgen en dient uit te monden in ontwerpprincipes
- Elke deelvraag dient een eigen zoekboom en conclusie te krijgen
- De deelvragen dienen gebruikt te worden om een conclusie te geven op de hoofdvraag

In deze literatuurstudie wordt deelvraag 4 uitgewerkt: "Welke mogelijke conceptuele oplossingen zijn er?".

Methodieken

Bij de literatuurstudie wordt er gebruik gemaakt van een tweetal overkoepelende methodieken. Deze methodes zorgen ervoor dat het onderzoek methodisch en herleidbaar wordt uitgevoerd.

Literatuuronderzoek:

Het literatuuronderzoek wordt uitgevoerd om de deelvragen vanuit de probleemanalyse te beantwoorden. In deze datacollectie methode wordt er gebruik gemaakt van internetbronnen, boeken en verkregen online documentatie. Hier wordt desk- en fieldresearch voor uitgevoerd.

6.1 Deelvraag: Welke mogelijke conceptuele oplossingen zijn er?

In dit hoofdstuk wordt er gekeken naar verschillende conceptuele mogelijkheden om monitoren en logging in te richten. Om structuur aan te brengen in het hoofdstuk worden de concepten opgedeeld in subhoofdstukken. Op het moment dat de conceptuele mogelijkheden zijn beschreven worden er een aantal voorbeelden gegeven om het geheel minder abstract te maken. Deze deelvraag concludeert in ontwerpprincipes.

Best practices:

Wanneer er gekeken wordt naar monitoring bij organisaties, wordt er in ideale situatie gehandeld en gewerkt volgens best practices. Het doel van deze best practices is om ervoor te zorgen dat er gestroomlijnd tewerk gegaan wordt, waarbij er voorkomen dient te worden dat er na positieve intentie, negatieve gevolgen van projecten zijn. Dit onderdeel beschrijft volgens (Modi, 2019) een vijftal best practices waarnaar gekeken dient te worden om een monitoring strategie succesvol op te zetten bij een organisatie. Hieronder staat een opsomming, waarna de diverse onderdelen verder uit worden gewerkt.

1. Begrijp het IT-landschap
2. Evalueer en selecteer het juiste monitoringsproduct
3. Bedenk zakelijke vereisten
4. Bedenk en meet KPI's
5. Definieer rollen en verantwoordelijkheden

[1]. Begrijp het IT-landschap

De eerste fase van het definiëren van een strategie is het opzetten van een roadmap, architectuurmodellen en knelpunten tussen de business en de IT-organisatie met een focus op de belangrijkste business processen. Daarnaast is het van belang om de juiste en belangrijkste use cases uit te werken. Een use case is hierbij een beschrijving van een persoon die het proces of systeem inzet om tot een doel te komen.

Mogelijke belangrijke vragen die gesteld kunnen worden om het IT-landschap inzichtelijk te maken zijn:

- Welke technologieën worden er gebruikt?
- Welke architectuur elementen of typen worden er gebruikt?
- Welke typen applicaties worden er gebruikt?
- Bestaan er SaaS of PaaS applicaties waardoor monitoring gelimiteerd kan raken?
- Bestaat er een roadmap met eventuele upgrades aan de systemen?
- Bestaat er een SIEM en zijn er kwetsbaarheden in de ingerichte SIEM?

[2]. Evalueer en selecteer het juiste monitoringsproduct

Er zijn inmiddels zo ontzettend veel producten die verschillende features leveren, waardoor het kiezen steeds lastiger wordt. Om het keuzeproces gerichter te maken kunnen de onderstaande categorieën een richtlijn bieden om de juiste keuze te kunnen maken.

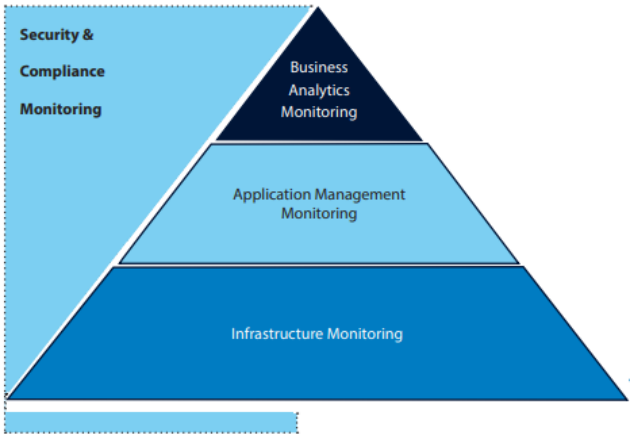
- Compatibiliteit
- Functies
- Integratie(mogelijkheden)
- Kosten

[3]. Bedenk zakelijke vereisten

De traditionele manier om monitoring requirements inzichtelijk te maken is om vanuit onderaan te beginnen, hierbij wordt ze zogenoemde 'bottom-up approach' gehanteerd. Het voordeel hiervan is dat alle technische requirements erg goed inzichtelijk gemaakt worden, voorbeelden hiervan zijn metrics omtrent Memory, Disk Space, CPU etc. Het nadeel hiervan is echter dat er vaak pas achteraf gerealiseerd wordt dat de gekozen oplossing niet op een lijn zit met de eisen en wensen van de business.

Om dit op te pakken kan er ook gekozen worden voor de zogenoemde 'top-down approach'. Hierdoor blijft de scope gericht op het doel van de business en wordt het niet uitgerekt door infrastructurele eisen en mogelijkheden. Ook wordt de beschreven mismatch tussen business en technologie voorkomen, wordt haalbaarheid met de daarbij komende knelpunten vroegtijdig inzichtelijk en zorgt dit tot slot voor dat alle betrokken partijen op een lijn zitten over de oplossing (Modi, 2019). Deze oplossing past zo ook beter bij de IT-roadmap.

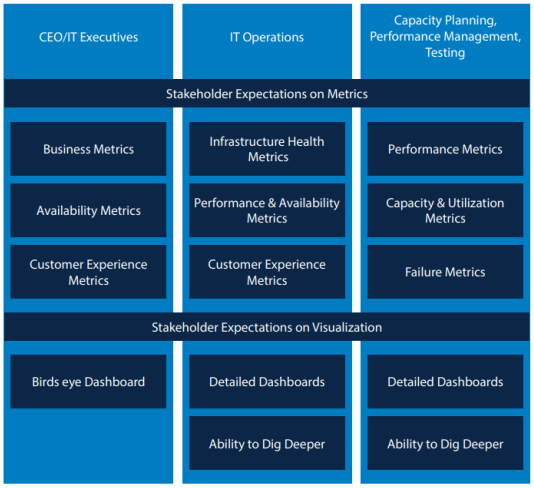
Rechter afbeelding visualiseert deze manier van denken/ aanpak:



Figuur 14 Het oppakken van Top-Down monitoring (Modi, 2019)

[4.] Bedenk en meet KPI's

Met de constante uitbreiding van infrastructuren en systemen wordt de (IT)omgeving van de organisatie steeds complexer. Het opzetten van een monitoringsoplossing draagt hieraan bij, zowel op positieve als negatieve wijze. Hoewel er namelijk data inzichtelijk wordt gemaakt, komt er wel weer extra data bij in de organisatie. Een belangrijke uitdaging hierbij is het versimpelen van de data, waarbij het doel is om dit leesbaar te maken voor gebruikers (en vooral beheerders). Een goed startpunt is het inzichtelijk maken wat de eisen en wensen zijn van de diverse betrokken partijen. Hierna kunnen de metrics worden vastgesteld en kan er onderscheid gemaakt worden tussen verschillende oplossingen om deze metrics inzichtelijk te maken voor de verschillende belanghebbenden.
De afbeelding illustreert deze scheiding in mogelijkheden en is ingedeeld per stakeholder. De belanghebbende staat bovenin aangegeven, waarna gevisualiseerd is welke metrics er per stakeholder van belang is. Tot slot wordt aangegeven welke oplossing het beste aansluit bij verschillende stakeholders. Dit model dient als voorbeeld om KPI's op te stellen.



Dit draagt bij aan: REQ-B-07

Figuur 15 Het identificeren van KPI's gebaseerd op individuele stakeholders (Modi, 2019)

[5]. Definieer rollen en verantwoordelijkheden

Het definiëren van rollen en verantwoordelijkheden is vooral van belang nadat de monitoringsoplossing geïmplementeerd is. Door het inrichten van deze twee aspecten wordt er gegarandeerd dat het monitoringsproject niet strand in de nazorgfase maar dat het daadwerkelijk geïntegreerd wordt in de organisatie. Kortom dienen alle genomen stappen die continue werkzaamheden met zich mee brengen ingedeeld te worden. Het is hierdoor van belang dat de genomen stappen bijgehouden en niet vergeten worden op het moment dat ze uitgevoerd en 'voltooid' zijn (Modi, 2019).
Dit voldoet aan: REQ-U-04

Monitoring:

Nu de best practices geformuleerd zijn, kan er worden ingedoken op de 'daadwerkelijke concepten' omtrent monitoring. In de komende subhoofdstukken wordt ingegaan op deze concepten, waarbij begonnen wordt met monitoring: *"Monitoring is de continue of regelmatige observatie van een informatiesysteem of component daarvan, en het vastleggen van alle onregelmatigheden"* (Boer, 2015).

(Information Security) Continuous Monitoring (ISCM):

ISCM is het doorlopend bewust te blijven van informatiebeveiliging, kwetsbaarheden en bedreigingen om beslissingen te nemen over risicobeheer van organisaties. De termen "continu" en "doorlopend" in deze context betekenen dat beveiligingscontroles en organisatorische risico's beoordeeld en geanalyseerd worden met een frequentie die voldoende is om risico gebaseerde beveiligingsbeslissingen te ondersteunen, om zo de informatie van de organisatie adequaat te beschermen (NIST, 2021).
Monitoring wordt kan worden opgesplitst in een tweetal onderdelen, namelijk: Logging en rapportage.

Logging:

Het voorzien van logs in datalijsten van events. Deze vormen de basis voor effectieve monitoring, welke vervolgens als output een (gerichte) management rapportage levert. Logs kunnen zowel input als output zijn van monitoring. In het geval van een output is er vaak sprake van verdere analyse. Logging is geen auditing, hier wordt onderling ook onderscheid tussen gemaakt.

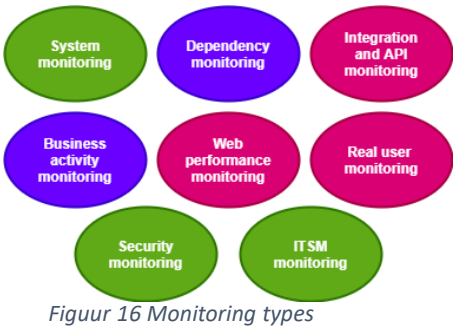
- Logging betreft de geproduceerde logs door systemen, user applicaties, OS-componenten. Deze worden vaak gedefinieerd als 'devices' (apparaten) of componenten.
- Auditing betreft de geproduceerde logs door trusted components, de kernel is hier een voorbeeld van (Boer, 2015).

Rapportage:

Het genereren van rapporten, welke de status weergeven van de IT-controlesystemen, die ontwikkeld zijn om redenen van compliance en kunnen ingezet worden voor risico management. Rapporteren wordt zowel gebonden aan monitoring als logging, omdat de bron van de gegenereerde rapporten op de output van beide kan zijn gebaseerd (Boer, 2015). Monitoring wordt vaak onderverdeeld in verschillende typen monitoring, maar er bestaat geen vastgelegde, vooraf gedefinieerde en leidende lijst. Het is echter wel verstandig om hier onderscheid in te maken om het beter te kunnen beheren (Raza M. , 2020). Daarnaast heeft monitoring ook een grote overlap/ correlatie met andere disciplines. Onderdelen die hierbij ter sprake komen zijn ITOM (IT Operations Management), SIEM (Security Information and Event Management, Security Orchestration, Automation, Response, OI (Operational Intelligence) en nog veel meer (Splunk, 2021). Hieronder worden de verschillende typen van monitoring beschreven en toegelicht.

Monitoring types

Er bestaat geen officiële lijst van verschillende soorten typen monitoring. Toch is het verstandig om onderscheid te maken tussen diverse soorten, om het concept verder op te delen. Als dit niet wordt gedaan, wordt monitoring vaak als een te groot en log concept opgepakt en kunnen belangrijke aspecten achterwege gelaten worden.
Monitoring kan op verschillende onderdelen worden ingezet om strategisch inzicht te krijgen in de organisatie en gaat vaak verder dan het monitoren van infrastructuurcomponenten. Rechterafbeelding geeft weer welke typen er bestaan, als er onderscheid gemaakt moet worden tussen de verschillende soorten (Raza M. , 2020):



Figuur 16 Monitoring types (Raza M. , 2020)

System monitoring:
Het evalueren van de performance of infrastructuurcomponenten van de fysieke laag van het netwerk. Elke server wordt apart gemonitord en de opgehaalde informatie van nodes wordt verder geanalyseerd om te kunnen evalueren wat de impact op het netwerk is. Het identificeren van hardwarecomponenten kan hiermee worden gedaan, bevindingen kunnen op deze manier goed aangepakt worden.

Dependency monitoring:
Applicaties op gedistribueerde IT-infrastructuren kunnen afhankelijk zijn van verscheidene netwerk nodes, services of componenten. Deze afhankelijkheden (dependencies) worden in kaart gebracht en geëvalueerd. Op deze manier kan performance gemeten worden, doordat inzichtelijk wordt gemaakt welke resources er gebruikt en verbruikt worden. Door afhankelijkheden inzichtelijk te maken en te monitoren kan er inzichtelijk worden gemaakt wat de onderliggende architecturale afhankelijkheden zijn tussen applicaties, hardware en services.

Integration and API-monitoring:
Integratie monitoring wordt gebruikt om performance, beschikbaarheid en uptime te monitoren van third-party integraties op applicaties.

Business activity monitoring:
Het monitoren van business activiteit staat recht tegenover het monitoren van de IT-infrastructuur. Er bestaat een correlatie tussen deze twee aspecten. Doordat het gebruik van resources bijvoorbeeld gemonitord wordt, kan de business bepalen wat de gerelateerde business activiteiten moeten zijn. Hiervoor worden vaak metrics gebruikt en ingezet, deze metrics zijn er dan voor om inzicht te bieden in financiële, security, operationele of technologische performance aspecten.

Web performance monitoring:
Web performance monitoring vindt plaats op basis van web-based services, zoals websites. Daarbij ligt de focus op hoe bepaalde onderdelen van websites reageren op de gebruikersverzoeken, met daarbij weer een focus op client-side netwerken. Het meten van deze performance is vaak gericht op laadsnelheid, het versturen en ontvangen van data en de bijkomende foutmeldingen, foutmeldingen tijdens het laden etc. Met de focus op cybersecurity en het verhogen van het beveiligingsniveau zal dit type monitoring niet heel toepasbaar zijn.

Real user monitoring:
Het bijhouden van het aantal gebruikers dat zich per minuut of seconde begeeft op een pagina en voor hoelang deze gebruiker zich daar begeeft kan belangrijk zijn voor data-analyses. Met de focus op cybersecurity en het verhogen van het beveiligingsniveau zal dit type monitoring niet heel toepasbaar zijn.

Security monitoring:
De businesscontinuïteit kan aangetast worden op het moment dat er een aanval is op het netwerk. Op zulke momenten komt er vaak ook vreemd verkeer voor in het netwerk. Door hier specifiek op te monitoren kunnen dit soort vreemde activiteiten getraceerd, geanalyseerd en geregistreerd worden. Dit kan vaak gerealiseerd worden door het inzetten van een oplossing gebaseerd op AI (kunstmatige intelligentie).

ITSM-monitoring:
Het monitoren van IT en Service Management kan op vele manieren worden gedaan, waarbij een meer gebruikelijke en breder inzetbare manier is: Het monitoren van metrics en KPI's. Door deze twee aspecten in te zetten om ITSM te monitoren kan de performance van ITSM geëvalueerd worden en kan hier gepast op gehandeld worden vanuit de business (Raza M. , 2020).

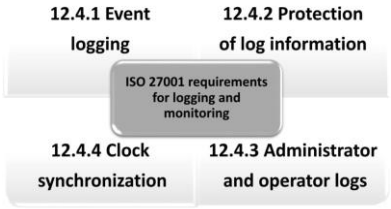
Monitoring standaarden

Monitoring kan worden gestandaardiseerd door gebruik te maken van standaarden. Vanuit de contextanalyse (RV-02 & 03) kan gesteld worden dat er een focus ligt op de ISO-standaarden. De ISO-standaarden hebben een focus op security, waarbij deze standaarden aangeven welke doelen behaald moeten worden om te voldoen aan de standaard(en).

ISO 27001:

"ISO 27001 was developed to help organizations, of any size or any industry, to protect their information in a systematic and cost-effective way, through the adoption of an Information Security Management System (ISMS)." (27001 Academy, 2021)

ISO 27001 sectie A.12.4 "Logging en Monitoring" beschrijft welke requirements er benodigd zijn om te voldoen aan deze standaard. Door deze sectie/ standaard te volgen wordt log integriteit behaald en gegarandeerd.



Figuur 17 ISO 27001 A.12.4 Logging and monitoring requirements (Segovia, 2015)

Event logging:

Registreer informatie over toegang en acties van gebruikers, fouten, gebeurtenissen, etc. in informatiesystemen. Als er meerdere applicaties zijn, kan het interessant zijn om de logboeken die door elke applicatie zijn gegenereerd, naar een centrale server te sturen. Om dit te doen, kan er een Syslog-server geconfigureerd worden, of kan een SIEM-oplossing ingezet worden. Hierdoor worden alle logboeken op een unieke server gecentraliseerd.

Protection of log information:

De logs moeten worden beschermd, omdat ze niet verwijderd of gewijzigd moeten kunnen worden door onbevoegd personeel of een kwaadwillende. Als een aanvaller toegang krijgt tot een niet-geautoriseerd systeem, verwijdert deze persoon over het algemeen alle informatie die in de logboeken is gegenereerd om bewijs te verwijderen van alle acties die zijn uitgevoerd. Daarom moeten er regels worden opgesteld om het bewerken van logbestanden alleen toe te staan door specifieke medewerkers. Toegang tot de systemen en de controle hiervan dienen uiteraard versterkt te worden.

Administrator and operator logs:

Privileges van beheerders en operators van systemen verschillen vanzelfsprekend van de normale gebruikersprivileges, beheerders kunnen meer acties uitvoeren op systemen dan gebruikers. In sommige gevallen wordt dergelijke (beheer)activiteit standaard niet geregistreerd, terwijl dit wel moet gebeuren. Als een aanvaller toegang krijgt tot een ongeautoriseerd systeem, zal deze aanvaller hoogstwaarschijnlijk proberen beheerdersrechten te verkrijgen en alle acties uitvoeren met de rechten van deze beheerder. Daarom moeten systemen informatie over alle gebruikers registreren, ongeacht de rechten die ze op de systemen hebben of de status die ze hebben binnen de organisatie.

Clock synchronization:

Alle systemen moeten worden geconfigureerd met dezelfde tijd en datum. Op het moment dat een incident zich voordoet en er een traceerbaarheidstest uitgevoerd gaat worden, kan dit ingewikkeld worden als niet alle betrokken systemen dezelfde (tijd)configuratie hebben. Daarom zou het ideale scenario zijn dat systemen een gesynchroniseerde tijd hebben door bijvoorbeeld tijdservers in te zetten. Dit kan ook geautomatiseerd worden door een bijvoorbeeld een NTP (network time protocol) -server in te zetten (Segovia, 2015).

Dit voldoet aan: REQ-U-09

Chief Information Security Officer (CISO):

Volgens (Bresser, 2020) kan het tactische volwassenheidsniveau alleen behaald worden op het moment dat er gekeken en voldaan wordt aan de ISO-27001 standaard. Hoewel deze standaard niet beschrijft dat er officieel een CISO aangesteld dient te worden, is het wel streng aanbevolen.

Vaak wordt er bij organisaties ook gesproken over het aanstellen van een Chief Security Officer (CSO), maar een CSO en een CISO verschillen toch echt van elkaar. Een CSO is verantwoordelijk voor het maken en uitvoeren van protocollen, standaarden, specificaties en richtlijnen. Hierbij is het ook belangrijk dat er (security) awareness wordt opgewekt bij medewerkers. Een CSO heeft daarnaast als het ware een breder takenpakket, omdat het ook gericht is op externe aspecten. Hierbij hoort bijvoorbeeld het onderhouden en beheren van relaties met leveranciers, securitymanagers en het afstemmen van compliance audits met externe partijen (Glen, 2020).

Het beschrijven van een CISO kan op een korte wijze gedaan worden door te kijken naar het begrip 'Cyber Security'. Cyber Security, privacy van gegevens, incident management, risicomanagement en het beheren van toegang tot systemen met daarbij de focus op data en informatiesecurity zijn allemaal dagtaken van een CISO.

Als de vergelijking in het kort moet worden opgesomd, kan gesteld worden dat een CSO als het ware verantwoordelijk is voor de fysieke beveiliging en veiligheid van medewerkers en de CISO verantwoordelijk is voor de beveiliging van data en systemen. Over het algemeen heeft een CISO ook een achtergrond in ICT (Fruhlinger, 2018).

In de context van dit project kan een CISO ervoor zorgen dat Oosterberg de onderstaande aspecten beter kan beheren, door verantwoordelijkheden te hebben over de volgende functionele domeinen in de organisatie (Raza M. , 2020):

- End-to-End Security Operations
- Compliance
- HR Management
- Stakeholder Onboarding
- Documenting
- Disaster Recovery & Business Continuïteit
- Cyber Security

Het afhandelen van incidenten volgens ISO 27001 A.16:

Wanneer een mogelijk incident zich voordoet, is het wel van belang dat er bekend is hoe deze op juiste wijze kan worden afgehandeld. Dit onderdeel ligt dit kort toe, door de vijf stappen te beschrijven over 'hoe dit te doen'.

Het afhandelen van security incidenten wordt gebaseerd op een vijftal verschillende stappen:

- Notificeren van het incident/ communiceren over het incident
- Classificeren van het incident (door een technisch specialist)
- Behandelen van het incident
- Afsluiten van het incident
- Registreren van het incident in een kennisdatabank

Figuur 18 Security incidenten behandelen in 5 stappen (Segovia, 2016)

Het classificeren van incidenten volgens ISO 27001 A.16:

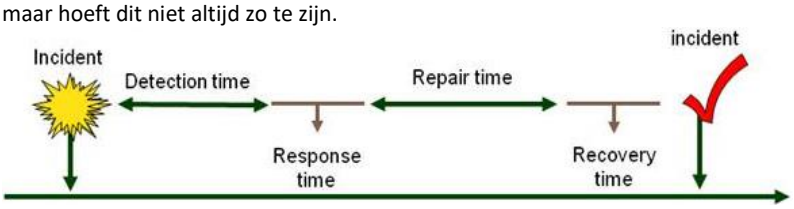
Classificeren van security incidenten kan worden gedaan door de impact af te leggen met de urgentie, hierdoor kan prioriteit bepaald worden. Het classificeren kan hierbij bijvoorbeeld gedaan worden door een priority matrix te gebruiken. Rechter afbeelding geeft hier een voorbeeld van weer:

Urgency \ Impact	High	Medium	Low
High	1	2	3
Medium	2	3	4
Low	3	4	5

Figuur 19 Priority matrix voorbeeld (Segovia, 2015)

Incidenten:

ITIL definieert een incident als ongeplande onderbreking of verlaging van kwaliteit van een IT-service (BMC Software, 2020). Het is zaak om één of meerdere incidenten of calamiteiten op de juiste wijze op te pakken. Want een incident heeft impact op het systeem, hoewel de impact kan variëren per gebruiker. Daarnaast kan een incident zichtbaar zijn voor de gebruiker, maar hoeft dit niet altijd zo te zijn.



Figuur 20 Uitgebreide incident lifecycle (Meenarani Rani, 2019)

Op het moment dat de juiste monitoring oplossing en het vastleggen van KPI's (Key Performance Indicators) van applicaties, systemen of het functioneren van de IT-afdeling niet aanwezig is, dan resulteert dit in een reactieve IT-omgeving waarbij de incidenten vanuit gebruikers komen.

Dit draagt bij aan: REQ-B-06, REQ-B-07

ISO/IEC 20000:

ISO/IEC 20000 is de internationale standaard die gespecificeerd is voor ITSM (IT Service Management). Deze standaard beschrijft een reeks aan managementprocessen die vorm geven aan een SMS (Service Management System) zodat services effectiever geleverd kunnen worden aan de business en haar consumenten. Daarbij kan ISO/IEC 20000 worden ingezet om een SMS op te zetten, te implementeren, te onderhouden en te verbeteren (ISO.org, 2021). Het inzetten van een SMS is een strategisch besluit voor een organisatie en deze beslissing wordt hevig beïnvloed door de doelen van de organisatie. Door een SMS op te zetten kan monitoring ervoor zorgen dat er meer dan alleen technische componenten worden gemonitord.

ISO-standaarden alternatief: COBIT

Toch kan er een andere belangrijke monitoringstandaard overwogen worden, namelijk de COBIT-standaard. COBIT (Control Objectives for Information and Related Technologies) is een IT-management en Governance framework. Het framework levert implementeerbare instrumenten over informatie technologie die worden opgesteld als IT-gerelateerde processen die de business ondersteunen. Een belangrijk verschil is dat ISO een focus heeft op (information) security en hoewel COBIT dit ook doet, heeft COBIT een bredere scope en een focus op governance (27001 Academy, 2016). Governance is het leveren van structuur om IT strategie op een lijn te krijgen met de business strategie (CIO, 2017).

Ondanks de verschillen in de scope van de standaarden, zijn er belangrijke overeenkomsten:

1. Gestuurd door doelen
2. Proces georiënteerd
3. Het gebruik van steunmethodieken/ instrumenten

COBIT kan profijt leveren wanneer een organisatie de IT-omgeving meer op een lijn wil laten komen met de business. Dit kan ervoor zorgen dat bedrijfsdoelstellingen efficiënter behaald worden. Het COBIT-framework is zeer effectief in het opstellen van werkprocessen en laat organisaties bedrijfsdoelstellingen niet alleen beter behalen, maar ook identificeren.

Verdere voordelen van COBIT is het feit dat dit framework maatregelen en processen introduceert die identificatie en eliminatie van IT-risico's makkelijker maakt.

COBIT kan ook parallel met ISO worden ingezet, hierbij kan COBIT zorgen voor het effectief gebruiken van informatie en kan ISO zorgen voor de integriteit en beschikbaarheid van data en meet/ controle-instrumenten.

Kortom is COBIT meer gericht op processen, strategieën en de business. In het kader van best practices in de monitoringwereld kan het interessant zijn om COBIT te onderzoeken, te overwegen en eventueel te implementeren.

Monitoring strategie

Naast het volgen of hanteren van monitoring standaarden is het van belang dat er wordt gekeken naar het toepassen van een monitoring strategie. Effectief monitoren en beheren van events door het opzetten van een managementstrategie zijn van essentieel belang bij het succesvol opzetten van monitoring in een organisatie. Een monitoring strategie is een gestandaardiseerde set van procedures die ervoor zorgen dat data opgehaald, geanalyseerd, voorspeld en gerapporteerd kan worden. Dit wordt gedaan op basis van de performance van de infrastructuur en haar applicaties, op zowel reactieve als proactieve manier, om zo de beschikbaarheid van deze componenten te verhogen (Meenarani Rani, 2019).

Op het moment dat er in een organisatie geen gecentraliseerde monitoring oplossing is, zijn organisaties volledig reactief. In zo'n situatie is een organisatie afhankelijk van de meldingen van gebruikers en niet gefocust op de performance van de systemen. IT-medewerkers/ afdelingen dienen monitoring op een hoger niveau in te zetten. Er moet meer dan alleen de infrastructuur gemonitord gaan worden, er dient namelijk ook gekeken te worden naar de business service performance. Dit houdt in dat er begrepen wordt wat de doelen van de organisatie zijn en op welke wijze de beschikbaarheid van de applicaties en componenten hieraan bij kunnen dragen (Meenarani Rani, 2019).

Monitoring protocollen

Vanuit best practices kan monitoren het beste worden opgebouwd vanuit het component niveau (Boer, 2015). Component monitoring kan in dit geval worden gedaan door het toepassen van een of meerdere monitoringsprotocollen. Netwerk monitoring protocollen zijn ontworpen om data te kunnen traceren en vervolgens te kunnen laten rapporteren. Over het algemeen worden deze protocollen toegepast als er een aspect in een client- naar hostnetwerk bekeken dient te worden. De verkregen data kan vervolgens weergegeven worden middels een GUI, zodat systeembeheerders deze informatie kunnen toepassen om het netwerk beter te beheren (LiveAction, 2021). Protocollen zorgen er dus voor dat een log bericht van A naar B kan worden getransporteerd en zorgen er zo voor dat de integriteit wordt gewaarborgd (Boer, 2015).

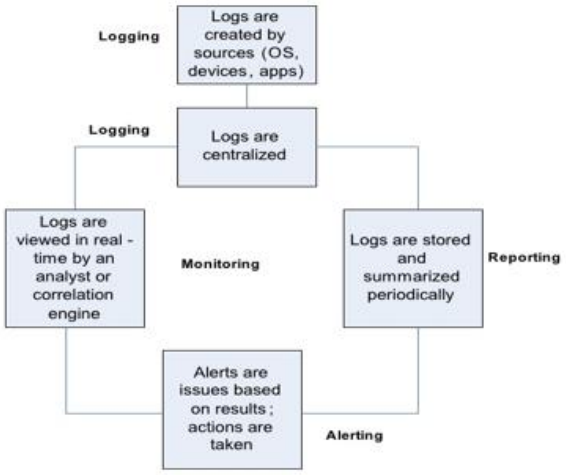
Er zijn verschillende soorten protocollen, waarvan sommigen meer gebruikt worden dan anderen. Het toepassen van deze protocollen wordt gedaan door applicaties of platformen in te zetten. De meest gebruikte protocollen zijn SNMP, ICMP, Syslog UDP, Syslog TCP, (S)FTP, CDP en Windows Event Log (Tek-Tools, 2020). Een goed en wellicht het belangrijkste voorbeeld is hierbij SNMP, ofwel het Simple Network Management Protocol. Dit application-layer protocol is het belangrijkste standaardprotocol als het gaat om het concept 'monitoring' (Boer, 2015). SNMP kan worden ingezet om data zoals CPU-load, bandbreedte, netwerksnelheden en vertragingen op te halen van componenten zoals WLAN-controllers, servers, routers, printers enzovoorts. Een belangrijk onderdeel van SNMP is de Management Information Base (MIB), dit is een catalogus van objecten waar SNMP naar kan kijken om de status van apparaten te bepalen. Data die in deze MIB wordt gezet, wordt verkregen vanuit de SNMP-agents die op de beheerde apparatuur is geïnstalleerd (LiveAction, 2021).

Logging

Een traditionele monitoringsoplossing heeft Oosterberg al, dit wordt momenteel gedaan door PRTG in te zetten. Logging wordt echter op zeer minimale wijze ingezet, maar is toch een van de 'key-components' van monitoring, monitoring kan niet juist worden ingezet als logging niet wordt opgepakt. In dit onderdeel wordt het concept 'logging' behandeld en wordt er gekeken naar welke aspecten er bij logging komen kijken.

Log(s): Een log is hetgeen dat wordt gegenereerd als antwoord op bepaalde stimuli. Logs (of log messages) leveren informatie m.b.t. resource, applicatie, user en security management. Het is een verzamelnaam voor meerdere log messages m.b.t. een bepaalde gebeurtenis (event).
Log data: Log data is de inhoudelijke informatie van een log.
Recording: Het verzamelen van alle eventfields in een eventrecord
Eventrecord: een enkel event
Logging: Een korte beschrijving is de verzameling van eventrecords in logs, zoals .txt en .bin files. Verder kan ook hierbij een onderscheid gemaakt worden tussen 4 types van logging.
Security logging: Detectie en het nemen op actie op aanvallen.
Operational logging: Dit is het detecteren van fouten in het systeem en het analyseren van niet IT-zaken, zoals inzicht tonen in het aantal mensen dat een website heeft bezocht.
Compliance logging: Lijkt op security logging. Hierbij is er detectie van zaken waarbij de regels worden overtreden. Voorbeelden hiervan zijn system design, en ITIL-regelgeving.
Application debug logging: Dit is alleen actief als de applicatie niet juist functioneert.
Security incident: Het optreden van één of meerdere security events
Alarm/ Alert: Het nemen van een actie a.d.h.v. een event(log) (Boer, 2015).

Onderstaande afbeelding geeft weer wat een mogelijke processtroom is met de genoemde termen.



Figuur 21 Voorbeeld processtroom log managementcomponenten (Boer, 2015)

Log retention policy

Logging inzetten zonder hierbij een retentiebeleid op te stellen, heeft vaak het gevolg dat er een te grote hoeveelheid logdata komt en dit kan zo met gemak tot in de terabytes uitlopen. Om dit te voorkomen dient te technische voorziening juist geconfigureerd te worden, maar dan wel op basis van een log retentie beleid. In dit beleid staat hoelang welke soorten logs bewaard dienen te worden, op welke wijzen dit het beste gedaan kan worden en op welke medium deze data opgeslagen dient te worden. Het opstellen van een retentiebeleid dient gedaan te worden door alle belanghebbenden, vanuit zowel de business tot aan security en ICT-management (Boer, 2015).
In het log retentiebeleid dienen de volgende onderdelen aan orde te komen:

- Eisen m.b.t. naleving van regelgeving (compliance)
- Risicoprofiel van de organisatie
- Logbronnen
- Beschikbare opslagmedia

Een retentiestrategie kan er als volgt uit komen te zien:

- IDS + DMZ + online = 90 dagen
- Firewall + DMZ + online = 30 dagen
- Servers + intern + online = 90 dagen
- ALL = DMZ + archief = 3 jaar
- Kritisch + intern + archief = 5 jaar
- OTHER + intern + archief = 1 jaar (Boer, 2015)

Dit voldoet aan: REQ-B-06, REQ-U-03

Log acties op basis van kritische logs

In geval van een kritische incident of bevinding is het van belang dat er helder is welke stappen er ondernomen dienen te worden. In vergelijking met monitoringsstandaarden en best practices, bestaat hier geen officiële standaard voor (Boer, 2015). Onderstaande opsomming geeft een lijst van te nemen acties weer.

1. Identificeer welke log bronnen en geautomatiseerde tools ingezet kunnen worden tijdens de analyse
2. Kopieer log records naar een centrale locatie waar ze ingezien kunnen worden
3. Minimaliseer de bulk van logs door de routine en herhalende log entries te verwijderen (nadat bevestigd is dat deze niet van belang zijn)
4. Stel vast dat de datum en tijd (timestamps) van de logs betrouwbaar zijn, tijdzones worden vaak uit het oog verloren
5. Focus op de meest recente veranderingen, mislukkingen, fouten, status veranderingen, toegang en beheer events en overig verdachte events
6. Ga 'terug in de tijd' om de acties opnieuw uit te voeren, van zowel voor als na het incident
7. Relateer verschillende log activiteiten aan elkaar om zo een totaalplaatje te krijgen
8. Bedenk wat er mis is gegaan, hoe een incident zich voor heeft kunnen doen en bekijk de logs om de theorieën te bevestigen of juist uit te sluiten (Boer, 2015).

Toch kan het zo zijn dat er in het geval van 'niet kritische logs' actie ondernomen dient te worden. Hiervoor is het opstellen van een actieplan aanbevolen. Onderstaande tabellen geven een kort voorbeeld over hoe een actieplan eruit kan komen te zien:

Log	**Hoog verbruik bandbreedte**
Indicatie	Samenvatting
Actie trigger	Een lange logfile waarin het gebruik van bandbreedte is geregistreerd kan resulteren in een top drie van gebruikers, die tezamen 90% van de beschikbare bandbreedte in beslag nemen, dit kan leiden tot een disciplinaire maatregel

Tabel 6 Actieplan voorbeeld 1 (Boer, 2015)

Log	**Simpele inbraakpoging**
Indicatie	Trend
Actie trigger	Een groei kan duiden op een serieuze inbraakpoging

Tabel 7 Actieplan voorbeeld 2 (Boer, 2015)

Log	**Succesvolle logins**
Indicatie	Gecorreleerd
Actie trigger	Een succesvolle login na een reeks van niet-succesvolle logins, kan duiden op een brute force password aanval

Tabel 8 Actieplan voorbeeld 3 (Boer, 2015)

Dit voldoet aan: REQ-U-03

Logs analyseren

Inmiddels zijn er meerdere methoden, standaarden en protocollen beschreven over het inzichtelijk krijgen van logs. Voordat er op het onderdeel 'rapporteren' wordt gedoken, is 'hoe te analyseren' nog wel van groot belang. Het analyseren van logs, met daarbij best practices en standaarden worden in dit onderdeel toegelicht.

Organisaties die hun cybersecurity willen verbeteren zullen log analyse mogelijkheden in moeten richten. Organisaties die logs effectief kunnen monitoren en kunnen analyseren zorgen ervoor dat het netwerk beter beveiligd wordt en daarmee moeilijker binnen te dringen is. Door het inrichten van verbeterde cybersecurity, zorgt een organisatie er tot slot ook voor dat er niet alleen wordt voldaan aan regelgeving en richtlijnen, maar dat de frequentie van potentiële aanvallen verminderd wordt (Sumo logic, 2021).

Het verhogen van cybersecurity d.m.v. het inzetten van monitoring kan volgens (Sumo logic, 2021) worden gerealiseerd door de volgende richtlijnen te hanteren:

- ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls
- PCI DSS V3.1 (Parts 10 and 11)
- NIST 800-137 Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations

Bij het verhogen van cybersecurity d.m.v. monitoring is het van belang dat eerst gekeken wordt welke logs van belang zijn. Logs kennen onderling, net als bij monitoring, ook onderscheid in een aantal types. Onderstaande opsomming verdeeld volgens (Sumo logic, 2021) een aantal type logs:

System logs
- System activity logs
- Endpoint logs
- Application logs
- Authentication logs
- Physical security logs

Networking logs
- Email logs
- Firewall logs
- VPN-logs
- Netflow logs

Technical logs
- Http-proxy logs
- DNS, DHCP and ftp-logs
- Appflow logs
- Web and SQL-server logs

Cyber security monitoring logs
- Malware protection software logs
- Network intrusion detection system (NIDS) logs
- Network intrusion prevention system (NIPS) logs
- Data loss protection (DLP) logs

Het analyseren van logs kan worden gedaan door verschillende functies en methoden te gebruiken:
Normalisatie = Het verwerken van verschillende berichten tot hetzelfde formaat, dat leidt tot standaardisatie en overzicht in attributen van deze berichten.
Patroonherkenning = 'Machine learning', oftewel zelflerende machines/ technologie kan in worden gezet om patronen te herkennen in verschillende berichten. Hier wordt dan onderscheid gemaakt tussen interessante en oninteressante berichten. Deze oninteressante berichten worden meestal geclassificeerd als routine en leveren net als de interessante berichten alleen een melding als er een abnormaliteit wordt gedetecteerd.
Classificatie en tagging = Het groeperen van dezelfde typen berichten, hierdoor kunnen dezelfde berichten beter getraceerd worden en kan data op andere manieren gefilterd worden.
Correlatieanalyse = Deze analyse kan worden ingezet als de berichten uit diverse bronnen komen, waarbij het de bedoeling is dat er overeenkomsten gelegd kunnen worden tussen berichten vanuit verschillende systemen. Hierdoor kan men erachter komen dat individuele systemen gelinkt zijn aan dezelfde gebeurtenis (Sumo logic, 2021). Technische voorzieningen hebben over het algemeen standaard analyse-methodieken als ingebouwde functionaliteit.

Relevante log technieken

Een mogelijke technische oplossing om logging op te pakken is het inzetten van een Syslog server of het opzetten van een SIEM-oplossing. In dit onderdeel worden beide onderdelen toegelicht en vergeleken.

Syslog:

Syslog is een log managementprotocol. Syslog zorgt ervoor dat netwerkapparaten berichten en gebeurtenissen kunnen versturen. Om dit te kunnen realiseren, zorgt Syslog ervoor dat er een standaardformaat is dat alle applicaties en apparaten kunnen gebruiken. Een Syslog-bericht is altijd opgedeeld in de volgende drie onderdelen:
- Header, Structured data, Message

Wanneer een Syslog vergeleken wordt met een (event)log, zijn deze vaak versimpelde logs op basis van specifieke gebeurtenissen (events).

Een Syslog server wordt gebruikt en toegepast om alle Syslog-berichten op een centrale plek op te halen. Bij een Syslog server zijn er ook onderdelen die geautomatiseerd kunnen worden, zoals het berichtgeven naar systeembeheerders op het moment dat er een kritieke log langskomt (Dnsstuff, 2020).

SIEM:

Security Information Event Management (SIEM) is een systeem dat bestaat uit log analyse producten en software, ontwikkeld om organisaties een complete weergave te bieden van alle netwerkactiviteit. Een SIEM voegt meerdere losse functionaliteiten samen tot een overkoepelend geheel.
SIEM wordt vaak gecategoriseerd door de volgende eigenschappen:
Inzichtelijkheid: Ingebouwde dashboards met volledig inzicht in actuele en historische data
Centralisatie: Logs met daarbij alle belangrijke contextuele data worden opgeslagen en benaderd op een centrale locatie
Ordelijkheid & uniformiteit: Alle opgehaalde logs worden omgezet tot een duidelijk overzicht, voor gemakkelijk leesbare weergaves en inzichten
Correlaties: Event logs worden vergeleken door AI, algoritmes, regels, statistieken en real-time data
Alerting: Potentiële kwetsbaarheden worden d.m.v. alerts naar belangrijke partijen gestuurd
Prioriteren: Potentiële beveiligingsissues krijgen prioriteiten a.d.h.v. severities/ belangrijkheid
Rapportages: Rapportages kunnen automatisch worden opgeleverd voor opvolgingsdoeleinden en inzichten

Wat levert een SIEM-oplossing nog meer?

Een SIEM softwaresysteem voegt als het ware een drietal security tools samen in een pakket. Dit zijn:

- Security Event Management (SEM): Het samenvoegen van logbestanden van meerdere systemen om zo te zorgen voor overzicht m.b.t. beveiliging van de omgeving. Dit is met name gericht op securityspecialisten en niet zozeer op systeembeheerders.
- Security Information Management (SIM): Het verzamelen, monitoren en analyseren van data van computers. SIM pakketten hebben over het algemeen geïntegreerde functionaliteiten om geautomatiseerde meldingen te geven als er een gemonitord netwerkcomponent aangetast is. SIM-tools helpen securityspecialisten om 'incident-response' te automatiseren en daarnaast accurate rapporten te leveren.
- Security Event Correlation (SEC): SEC-software wordt gebruikt om door grote hoeveelheden van logs te spitten en hier correlaties en verbindingen uit te halen. Dit is gericht op events die mogelijke security risico's vormen (Sumo Logic, 2021).

Wat is het verschil tussen een Log Management Systeem (LMS) en SIEM?

Een SIEM-oplossing verschilt van een (Sys)Log Management Systeem (LMS). Een LMS is een softwaresysteem dat logbestanden van meerdere netwerkcomponenten samenvoegt en op centrale locatie opslaat. Een LMS-tool is het meest vergelijkbaar met een SEM-oplossing en een LMS-tool kan worden ingezet als er logs opgehaald moeten worden en deze op een centrale plek bekeken moeten worden door een systeemanalist. Alles wat een LMS heeft, heeft een SIEM-oplossing ook (Sumo Logic, 2021). De meest opvallend overeenkomsten zijn:

- Log datacollectie
- Efficiënt behouden van data
- Log indexering en zoekfunctionaliteiten
- Rapporteren op basis van performance, security of compliance

De meest opvallende functionaliteiten die een LMS niet kan bieden maar een SIEM-oplossing wel zijn:

- Bedreigingsdetectie en meldingen
- Event correlatie(s)
- Dashboard (inclusief real-time monitoring)

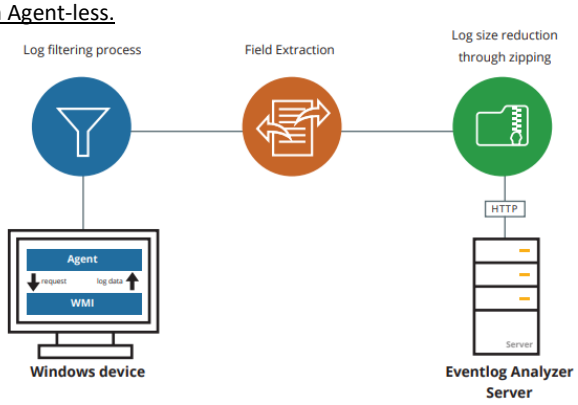
Bij SIEM-systemen staat security altijd voorop. (Sys)Log management wordt daarentegen alleen gebruikt om de log data op te halen. Log managementsystemen kunnen wel in worden gezet voor security doeleinden, maar dit zal altijd minder efficiënt zijn. Er zullen in zo'n geval meer operationele kosten worden gemaakt, omdat het systeem simpelweg niet alles levert wat een SIEM-oplossing wel doet. Automatiseren en analyseren zijn hier voorbeelden van. Log managementsystemen kunnen het beste in worden gezet om logbestanden op een plek te bewaren, maar op het moment dat deze logs gebruikt moeten gaan worden voor grote infrastructuren met analyses, kan daarvoor beter een SIEM-oplossing worden ingezet (SolarWinds MSP, 2020).

Een SIEM-oplossing is een samenvoeging van de drie beschreven functionaliteiten/ oplossingen en is zodanig meer gericht op security doeleinden. Op het moment dat een organisatie het doel heeft om logs op centrale wijze op te slaan en hier in eerste instantie alleen analyses op wil uitvoeren, dan kan een LMS een goede en goedkopere oplossing zijn. Op het moment dat een organisatie daarentegen een complexe ICT-omgeving heeft en deze wil beveiligen met de beste en uitgebreidere security-tools, dan kan er beter een SIEM-oplossing worden ingezet (Sumo Logic, 2021).

Niet alleen voor een SIEM-oplossing is de benodigde kennis bij medewerkers van belangrijk. Ook voor een SOC is het in gewenste situatie belangrijk dat er medewerkers zijn die hier tijd voor hebben en hier wellicht speciaal voor zijn aangenomen. *"Een SOC is een goed middel om zicht te houden op de beveiliging van bedrijfsinformatie en digitale dreigingen, maar het inrichten ervan kost tijd, geld en moeite. Om een SOC tot een succes te maken, is het van belang dat het SOC op een gecontroleerde wijze meegroeit met de behoefte aan zicht en grip op informatiebeveiliging vanuit de organisatie. Begin klein, maak de resultaten inzichtelijk voor de organisatie en gebruik een positieve ontvangst van deze resultaten als mogelijkheid voor een volgende stap in het groeiproces. Wees reëel in de planning, het groeipad en de invulling van een in te richten SOC. Besef daarbij: een SOC is een middel, geen doel."* (NCSC, 2021)

Wat is het verschil tussen agent-based en agent-less logs verzamelen?
Als het gaat om verzamelen van informatie, kunnen er twee methodieken worden gebruikt. Het is van belang dat bekeken wordt wat het verschil is tussen deze twee methodieken: Agent-based en Agent-less.

Agent-based logs verzamelen is erg handig als er gemakkelijk data verzamelt moet worden over een WAN en door een firewall. Een agent zorgt er in zo'n geval voor dat het netwerk beschikbaar wordt voor het verzamelen van logs. Hierbij kunnen agents er ook voor zorgen dat er gemakkelijker data van een apparaat in een DMZ gehaald kan worden. Tot slot zorgt een agent ervoor dat de CPU-load van een server lager wordt, wat resulteert in een hogere performance en een verlaagd aantal EPS (Events per second). Het verzamelen van logs wordt in dit geval gedaan door een oplossing op een server te zetten en het verkeer vanaf bijvoorbeeld een Windows-apparaat door te laten sturen naar deze server. Rechter afbeelding illustreert dit (ManageEngine, 2016).



Figuur 22 Agent-based logs verzamelen (ManageEngine, 2016)

Agent-less logs verzamelen wordt over het algemeen meer gebruikt. Agent-less creëert de volgende voordelen:

- Verlaagde implementatie en configuratie tijd – Omdat er geen agents geïnstalleerd hoeven te worden, hoeft de oplossing alleen maar geconfigureerd te worden en het configureren van deze setup kost geen moeite vergeleken met het volgen van een agent-based architectuur.
- Verlaagde beheer complicaties – Doordat er geen agents in het netwerk bestaan wordt het beheren van de monitoringinfrastructuur gemakkelijker. De meeste agent-less oplossingen hebben geïntegreerde zelf-monitoring mogelijkheden, waardoor het proces vergemakkelijkt wordt.
- Gemakkelijk om te upgraden – In een agent-based architectuur moeten alle agents bijgewerkt worden in geval van een update, bij agent-less is dit niet het geval.
- Minder fout tolerantie en impact – Op het moment dat er een fout ontstaat op een agent, wordt het gehele monitoringproces stopgezet op alle apparaten die verbinding hebben met die agent. Bij agent-less bestaat dit probleem niet (ManageEngine, 2021).

Security Operations Center (SOC)
Naast de al beschreven conceptuele en technische oplossingen, kan een Security Operation Center ook bijdragen aan het verhogen van het beveiligingsvolwassenheidsniveau van Oosterberg. Uit het rapport van Fox-IT blijkt dat het opzetten van een SOC ervoor kan zorgen dat Oosterberg de beschreven knelpunten op positieve manier kan oppakken (Bresser, 2020). Echter staat er niet beschreven wat een SOC is en hoe het ingezet kan worden om dit te behalen.

Wat is een SOC?
Een Security Operations Center is een gecentraliseerde functie in een organisatie die bestaat uit mensen, processen en technologieën om ervoor te zorgen dat de beveiliging van een organisatie gemonitord en verbeterd wordt. Hierbij worden cybersecurity incidenten voorkomen, gedetecteerd, geanalyseerd en gerapporteerd. Net als bij een SIEM-oplossing zal een SOC centraal staan in de organisatie en zo dienen als een vergaderpunt van de infrastructuur en informatie vanuit de assets uit de organisatie (McAfee, 2021).

Een succesvol werkend SOC kan alleen worden ingericht als er voldaan wordt aan een aantal criteria. Dit betreft de volgende eisen (NCSC, 2021):

- een beleid voor informatiebeveiliging met draagvlak door de hele organisatie
- accuraat overzicht van het applicatielandschap
- eigenaarschap van informatiesystemen
- recent uitgevoerde risicoanalyse
- samenwerking met de ICT-beheerorganisatie

De log-informatie die vanuit verschillende bronnen opgehaald en verwerkt zal moeten worden gedaan door een Security Information & Event Managementsysteem (SIEM) in te zetten.

Hoe komt een SOC tot stand?

Een SOC kan pas tot stand komen als er aan bovenstaand genoemde eisen wordt voldaan en er een gedegen monitoringsoplossing in de organisatie bestaat. Als een van deze onderdelen onvolledig ingezet is dan wordt het opzetten van een SOC afgeraden tot een later tijdstip (NCSC, 2021).

"Begin met het monitoren van eenvoudige technische zaken waar de organisatie baat bij heeft, bijvoorbeeld de log-informatie van de Active Directory, firewalls, antivirussoftware en webservers. Houd het eenvoudig en beperk de werkzaamheden tot de ICT-afdeling. Monitor alleen puur technische zaken.

Doe ervaring op met monitoren, registreren en afhandelen van incidenten. Ervaring opdoen met het hele proces van monitoren en incidentafhandeling is in het begin belangrijker dan het monitoren zelf. Bouw de monitoring gecontroleerd uit naar systemen die onderdeel vormen van de primaire bedrijfsprocessen. Maak afspraken met de ICT-afdeling over ICT-werkzaamheden als gevolg van die incidentregistratie. Richt u bij het monitoren niet op het per se willen inrichten van een SOC, maar richt u op wat voor de organisatie belangrijk en zinvol is." (NCSC, 2021)

Reporting

Het laatste onderdeel en resultaat van monitoring zijn samenvattingen en rapportages. Rapporteren (of Reporting) is belangrijk om een lijst te kunnen maken van de meest waardevolle rapportages. Onderstaande lijst geeft een opsomming van de voornaamste en belangrijkste rapporten:

Authentication & Authorization Reports	
Wat	Deze bevatten succesvolle en niet-succesvolle toegangspogingen tot systemen door gebruikers, zoals onder andere login pogingen, failures, logins op uitgezette (service) accounts, VPN-authenticatie, remote logins, beheeraccount toegang, meerdere (foutieve) logins
Hoe	Security analyst en CSO (Chief Security Officer)
Waarom	Dit is een kernactiviteit van informatiebeveiliging
Systems & Data Change Reports	
Wat	Deze bevatten systeem(configuratie), data- en beveiligingsveranderingen, dit betreft bijvoorbeeld veranderingen in users, groups, administratoraccounts, wachtwoord wijzigingen, netwerkservicewijzigingen en veranderingen in file-system configuraties
Hoe	Security analyst, CSO, systeembeheerders en incident beheerders
Waarom	Omdat ongeautoriseerde veranderingen veel schade aan de IT-voorziening kunnen toebrengen
Network Activity Reports	
Wat	Deze bevatten verdachte netwerkactiviteiten van systemen, dit betreft onder andere al het netwerkverkeer wat naar binnen en buiten gaat, zo wel op basis van een DMZ of interne netwerken. Ook betreft dit alle bestanden die gedownload zijn, een systeem die (te veel) verschillende protocollen gebruikt of de VPN-activiteit per gebruiker, met daarbij het aantal GB's op zowel bandbreedte als interne resources
Hoe	Security analyst, CSO, systeembeheerders en incident beheerders
Waarom	Dit moet omdat het netwerk de verbinding is tussen informatie (van de systemen) en de gebruiker en/ of hacker
Resource Access Reports	
Wat	Deze bevatten patronen over het gebruiken van databases, applicaties en systemen door gebruikers. Een aantal voorbeelden hiervan zijn bijvoorbeeld de access naar resources op kritische systemen buiten werktijden om, de toegang tot een netwerk of fileshare, een top aantal database gebruikers en een top aantal interne mailadressen die data naar buiten versturen in de vorm van bijlagen etc.
Hoe	Security analyst, CISO, resource eigenaren en incident beheerders
Waarom	Hierdoor kan misbruik van informatie opgespoord worden
Malware Activity Reports	
Wat	Deze bevatten kwaadwillige (software) activiteiten en gerelateerde gebeurtenissen. Dit betreft onder andere malware detectie (trends), antivirus meldingen, interne internetverbindingen naar bekende malware adressen en de meest recente/ voorkomende malware types
Hoe	Security personeel, CISO en incident beheerders
Waarom	Kwaadwillige software kan bedrijven veel schade laten oplopen
Failure & Critical Error Reports	
Wat	Deze bevatten opmerkelijke en significante (systeem)fouten m.b.t. informatiebeveiliging. Hierbij zijn de volgende voorbeelden van belang: Kritische fouten per systeem, applicatie of business unit met daarbij ook de crashes, shutdowns en restarts. Fouten in de back-up en capaciteitsmeldingen of bereikte limieten voor memory, disk, CPU en overige resources
Hoe	Security personeel, CISO en overige IT-medewerkers
Waarom	Vroegtijdige indicatie van potentiële informatiebeveiligingsdreigingen

Tabel 9 Belangrijkste rapporten (Boer, 2015)

Tips en valkuilen

Ter afronding van deze deelvraag, voordat de ontwerpprincipes worden geformuleerd, is het van belang dat er vaak voorkomende fouten worden beschreven. Hierbij is het van belang dat ook tips benoemd worden, om zo naast de best practices mogelijke problemen te voorkomen (Boer, 2015).

Logregels:

1. Verzamel alleen de data waarvan je weet dat je het gaat gebruiken
2. Bewaar data alleen zolang dit nuttig blijkt te zijn of zolang de wet dit voorschrijft
3. Log (met in achtneming van regel 2) zoveel mogelijk, maar filter alleen op alarms waarop actie ondernomen dient te worden
4. De beschikbaarheid van de monitoringomgeving dient niet hoger te zijn dan de mate van beschikbaarheid van algehele IT-omgeving, investeer daarom op gepaste wijze in oplossingen
5. De beveiliging van de monitoringomgeving dient niet hoger te zijn dan de mate van beveiliging van de algehele IT-omgeving, investeer daarom op gepaste wijze in oplossingen
6. Logbronnen, types en data veranderen continu. De organisatie dient mee te veranderen en zo regelmatig systemen en policies bij te werken

Algemene tips:

1. Verzamel niet te veel data als je deze niet op redelijke wijze kunt verwerken
2. Als er nooit iets interessants voorkomt, is dit wellicht juist interessant en waard om te onderzoeken
3. Real-time Intrusion Detection Systemen (IDS) werken niet als je niet ook Real-time beheer hebt
4. Het negeren van de bovenstaand beschreven logregels kan geclassificeerd worden als gevaarlijk en risicovol
5. Het besef dat de hoeveelheid log data toeneemt in relatie tot de toename aan belang bij IT voor de business is belangrijk
6. Monitoring opzetten zonder beleid, regels en policies zal leiden tot te veel data die te snel zal oplopen

Valkuilen:

1. Niet(s) loggen is niet verstandig en kan leiden tot serieuze gevolgen
2. Vaak wordt een monitoringsproces niet ingericht als een voorziening al operationeel is, hierdoor kan vervolgens niet proactief gemonitord worden
3. Log data dat te snel wordt weggegooid kan desastreuze gevolgen hebben voor risicomanagement
4. Log data dat te lang wordt bewaard is niet goed i.v.m. regulering, procedures en resource gebruik
5. Log data die te kort wordt bewaard is niet goed i.v.m. limieten aan forensisch onderzoek, risicomanagement en overige problematiek. Hier kan een strategie voor worden ingezet, waarbij (ten minste) de bron van de logs, netwerklocatie en de 'storage tier' wordt beschreven.
6. Prioriteren is belangrijk, maar doe dit pas als logging een tijd lang opgezet is. Vooraf bepalen van prioriteit zorgt voor een subjectief perspectief wanneer een calamiteit zich voor doet (Boer, 2015)

Conclusie

Omdat deze literatuurstudie bestaat uit één deelvraag en om de leesbaarheid van dit document te behouden, wordt de conclusie van deze deelvraag uitgewerkt in het volgende hoofdstuk 'Resultaten'. Hier worden de 9 thema's en bijbehorende resultaten van de thema's toegelicht (*Best Practices, Monitoring, Types, Standaarden, Strategieën, Protocollen, Loggen, Technische oplossing, Rapporteren*). De ontwerpprincipes worden hier ook genoteerd, waarna deze worden verwerkt tot een conclusie van het gehele rapport in het laatste hoofdstuk 'Conclusie'.

6.2 Resultaten

In dit onderdeel wordt er per thema beschreven wat de literatuur hierover stelt. Deze punten worden geconcludeerd in ontwerpprincipes en deze zullen per thema worden beschreven in het volgende hoofdstuk 'conclusie'. De bepaling over welke ontwerpprincipes wel of niet meegenomen zullen worden in het ontwerp, wordt gedaan in de ontwerp documentatie/ hoofdstukken (functioneel en technisch ontwerp).
De 9 thema's die worden behandeld zijn: *Best Practices, Monitoring, Types, Standaarden, Strategieën, Protocollen, Loggen, Technische oplossing, Rapporteren.*

Best Practices:
Volgens best practices te werk gaan is altijd een goed streven, maar niet altijd haalbaar. Toch zijn er een aantal interessante bevindingen gedaan die in zekere mate toepasselijk zijn op de casus van Oosterberg. Best practices beschrijven de gewenste manier van handelen en aanpak, waarbij het bij dit project zaak is dat er vooral grondig tewerk gegaan wordt. Hoewel monitoring over het algemeen strategisch aangepakt moet worden, is het zaak dat er vanuit het componentniveau opgebouwd wordt naar een uitgebreide monitoringoplossing. Op het moment dat gedaan is, kan er gekeken worden naar het uitbreiden richting de business. Hierbij is het de bedoeling dat KPI's worden ingericht en dat de business(eisen) en ICT meer op een lijn komen te zitten.

Monitoring:
Het concept monitoring bestaat eigenlijk alleen in Nederland en wordt wat minder gebruikt in de Engelstalige ICT-wereld. Het begrip 'Log management' wordt daarvoor gebruikt. Monitoring wordt veelal te kortzichtig ingezet bij organisaties en veel organisaties denken dat monitoring alleen maar in de vorm van een technische oplossing ingezet kan worden. Dit is echter niet het geval, monitoring kan breed worden getrokken over de gehele organisatie, vanaf de business, tot aan (web)applicaties en de infrastructuurcomponenten. Daarbij komt de 'komst van Cloud' ook nog eens om de hoek kijken, hoewel de Cloud volledig geïntegreerd en hedendaags is ondertussen. Het is van belang dat monitoring op het componentniveau wordt opgezet, waarbij er rekening wordt gehouden met uitbreidingen richting de overige beschreven lagen. Voor Oosterberg is dit ook van groot belang i.v.m. de verhoging van het beveiligingsvolwassenheidsniveau. Het niveau kan namelijk niet alleen verhoogd worden op het moment dat de techniek vooruitgaat, ook de mensen, processen en awareness dienen aangepakt te worden.

Types:
Monitoring kan worden opgedeeld in verschillende soorten types, hoewel hier geen officiële lijst voor bestaat. Het opdelen van monitoring kan bijdragen aan het inrichten van monitoren. Door monitoren als het ware op te delen, wordt ervoor gezorgd dat het concept monitoren minder log en groot wordt, waarbij er een focus komt te liggen op specifieke en belangrijke onderdelen. Hierbij sluiten de typen 'system, security en ITSM-monitoring' het beste aan bij dit project. System monitoring is hierbij het monitoren van de performance van de fysieke laag in het netwerk. Security monitoring is het monitoren van vreemd verkeer en gedrag om business continuïteit te garanderen. Tot slot is het monitoren van IT en Service Management van belang op het moment dat metrics en KPI's gemeten moeten worden. Hierdoor wordt er ook rekening gehouden met de business en wordt daarmee voldaan aan best practices in de monitoring wereld.

Standaarden:
Monitoring wordt gestandaardiseerd door gebruik te maken van standaarden. Deze standaarden beschrijven, definiëren en geven richting aan het monitoren door bijvoorbeeld inzichtelijk te maken wat er gemonitord dient te worden. Oosterberg geeft aan dat de ISO-standaarden prioriteit hebben en hierbij geven deze standaarden diverse belangrijke onderdelen aan. Deze onderdelen beschrijven hoe logs ingericht moeten worden, waarom dit op een bepaalde manier wordt gedaan en geven zo sturing aan ICT-afdelingen die dit willen gaan ondernemen. Oosterberg kan hierdoor profijt halen uit het toepassen van een standaard, waarnaast het bovendien ook nog bijdraagt aan het verhogen van het beveiligingsvolwassenheidsniveau. Door de ISO-27001 standaard te volgen, wordt log integriteit gegarandeerd. Op het moment dat de organisatie haar ICT-afdeling en de business meer op een lijn wil krijgen, dan kan het interessant zijn om te overwegen om de COBIT-standaard te gebruiken.

Strategieën:
Effectief monitoren en beheren van events door het opzetten van een managementstrategie zijn van essentieel belang bij het succesvol opzetten van monitoring in een organisatie. Een monitoring strategie is een gestandaardiseerde set van procedures die ervoor zorgen dat data opgehaald, geanalyseerd, voorspeld en gerapporteerd kan worden. Dit wordt gedaan op basis van de performance van de infrastructuur en haar applicaties, op zowel reactieve als proactieve manier, om zo de beschikbaarheid van deze componenten te verhogen. Daarnaast is het zo dat op het moment dat een organisatie geen gecentraliseerde monitoring oplossing heeft, de organisatie volledig reactief is. Er moet meer dan alleen de infrastructuur gemonitord gaan worden, er dient namelijk ook gekeken te worden naar de business service performance. Dit houdt in dat er begrepen wordt wat de doelen van de organisatie zijn en op welke wijze de beschikbaarheid van de applicaties en componenten hieraan bij kunnen dragen.

Protocollen:
In het kader van beveiliging en integriteit zijn protocollen van groot belang. Protocollen zorgen ervoor dat een log bericht van A naar B kan worden getransporteerd terwijl de integriteit van het logbericht wordt gewaarborgd. In verband met het starten op het componentniveau, is het voor Oosterberg van belang dat er in eerste instantie gekeken wordt naar het gebruiken en inzetten van het SNMP-protocol. SNMP kan worden ingezet voor alle infrastructuurcomponenten, zoals WLAN-controllers, routers en switches en dit komt zo overeen met de analyse van de kritieke assets van Oosterberg. Daarnaast is er al een Syslog mogelijkheid aanwezig, met wat uitbreidingen kan dit het beveiligingsniveau op korte termijn verhogen.

Loggen:
Loggen is een van de belangrijkste onderdelen van het succesvol kunnen monitoren, echter is zomaar gaan loggen een grote valkuil voor veel organisaties. Het is van belang dat er zoveel mogelijk wordt gelogd, maar alleen als het relevante data is. Loggen inzetten zonder hier een retentiebeleid voor op te stellen heeft desastreuze gevolgen voor organisaties en zodanig zal dit eerst opgesteld moeten worden. In dit retentiebeleid staat aangegeven hoelang welke soorten logs bewaard moeten worden en op welke wijze dit het beste gedaan kan worden. In een log retentiebeleid is het van belang dat de volgende onderdelen ten minste aan de orde komen:

- Eisen m.b.t. naleving van regelgeving (compliance)
- Risicoprofiel van de organisatie
- Logbronnen
- Beschikbare opslagmedia

Een van de onderdelen die daarnaast natuurlijk van groot belang is, is het actie kunnen nemen op basis van logs. Hiervoor zijn ook richtlijnen opgesteld, deze richtlijnen zijn als het ware een stappenplan om succesvol actie te kunnen ondernemen op basis van kritische logs. Daarnaast wordt het aangeraden om ook een kort en krachtig actieplan op te stellen voor de standaard meldingen en procedures i.v.m. de kans dat er mogelijke acties ondernomen moeten worden op basis van non-kritieke logs. Voor het analyseren van logs is het aanbevolen om de richtlijnen te volgen van ISO 27002:2013 en/ of van NIST 800-137.

Technische oplossing:
Omdat Oosterberg al acties ondernomen heeft op gebied van actueel monitoren (PRTG), is w.b.t. technische oplossingen vooral gekeken naar logging en zijn er als het ware tweetal conceptuele mogelijkheden beschreven. Allereerst is het mogelijk om een (Sys)Log Management Systeem in te richten (LMS). Deze oplossing heeft Oosterberg op het moment op minimale wijze ingericht en kan omschreven worden als een oplossing die gericht is op het effectief beschikbaar stellen van logsdata, waarbij er rapportages geleverd kunnen worden op basis van performance, security en/ of compliance. Daarnaast bestaan er SIEM-oplossingen, deze oplossingen leveren hetzelfde als een LMS met daarboven op functies zoals het detecteren van bedreigingen en hierover kunnen melden, event correlatie, herkenning en een dashboard inclusief real-time monitoring. Vanuit deze beschreven punten kan geconcludeerd worden dat een LMS goedkoper is en minder groot/ ingewikkeld is om in te richten. Daarnaast kan er ook geconcludeerd worden dat de eisen en wensen van Oosterberg beter aansluiten bij het inrichten van een SIEM-oplossing. Deze oplossing zal duurder zijn dan een LMS, maar omvat niet alleen alles waar Oosterberg naar opzoek is, maar houdt ook rekening met de toekomst. Een SIEM-oplossing kan worden opgezet op basis van agent-less en agent-based methoden. Beide methoden hebben duidelijke voordelen, maar in relatie tot de impact op technische performance zal een agent-based methode meer voordelen bieden voor Oosterberg. Als er echter volgens best practices wordt gehandeld dan kan er gesteld worden dat een agent-less SIEM-oplossing beter bij de organisatie past omdat dit rekening houdt met de mogelijke wijzigingen op technisch én procesmatige niveaus.
Ten slotte is een van de oplossingen, hoewel minder technisch, het inrichten en gebruiken van een Service Operations Center (SOC). Een SOC is een gecentraliseerde functie in een organisatie die bestaat uit mensen, processen en technologieën om ervoor te zorgen dat de beveiliging van een organisatie gemonitord en verbeterd wordt. Hierbij worden cybersecurity incidenten voorkomen, gedetecteerd, geanalyseerd en gerapporteerd. Net als bij een SIEM-oplossing zal een SOC centraal staan in de organisatie en zo dienen als een vergaderpunt van de infrastructuur en informatie vanuit de assets uit de organisatie. Indien de benodigde kennis en capaciteit bestaat binnen Oosterberg, kan een SOC zelf opgezet worden. Als dit niet het geval is, dan kan Oosterberg ervoor kiezen om een SOC uit te besteden. Op korte termijn zal het niet haalbaar zijn om een SOC te gaan gebruiken, maar kan het Oosterberg mooie kansen bieden in de toekomst, aangezien een SOC goed samengaat met een SIEM. Dit komt omdat een SIEM de werkzaamheden van SOC-medewerkers ondersteund door hen gedetailleerder en dieper op beveiligingsmaterie in laat gaan.

Rapporteren:
Afrondend is rapporteren ook van belang bij het inrichten van monitoren, maar is het aan Oosterberg in hoeverre dit wordt ingezet en gebruikt. Veel van de oplossingen hebben de technische functionaliteit om rapportages te genereren, maar dan is het wel van belang dat Oosterberg exact weet welke rapportages ze willen ontvangen. In de literatuurstudie is hier een opzetje voor gemaakt. Hiervoor zijn ook richtlijnen en het is aanbevolen dat deze in eerste instantie gevolgd worden. Rapporteren zal indirect bijdragen aan het beveiligingsvolwassenheidsniveau op het moment dat dit effectief wordt ingezet.

6.3 Conclusie

In dit hoofdstuk worden alle ontwerpprincipes weergegeven die uit de deelvraag/ literatuurstudie zijn gekomen. Deze ontwerpprincipes zijn de leidraad voor de ontwerpdocumenten in de ontwerpfase. Ontwerpprincipes worden ingedeeld per beschreven thema. Per ontwerpprincipe staat aangegeven aan welke requirements het principe bijdraagt. Omdat er nieuwe bevindingen zijn gemaakt tijdens de ontwerpfase wordt er een extra regel toegevoegd, deze 'ontwerpfase' categorie noteert de ontwerpprincipes die na de onderzoeksfase zijn gevonden.

Nr.	Req. Correl.	ALS	Onderneming	DAN	Actie	OMDAT	Beredenering
Best practices							
OP-01	REQ-U-08 REQ-U-09	*ALS*	Oosterberg monitoring wil inzetten om het beveiligingsvolwassenheidsniveau te verhogen	*DAN*	Dient er begonnen te worden op het componentniveau	*OMDAT*	Het volgens best practices (Boer, 2015) wordt aanbevolen om op het componentniveau niveau te beginnen
OP-02	REQ-B-08 REQ-U-09	*ALS*	Oosterberg het monitoringproject strategisch wil benaderen en in wil gaan zetten	*DAN*	Dienen er KPI's opgesteld en ingericht te worden	*OMDAT*	Dit zal leiden tot meetbare monitoringdata en te grote hoeveelheden log data voorkomen zullen worden, daarnaast resulteert dit in een proactieve ICT-omgeving
OP-03	REQ-B-05 REQ-U-09	*ALS*	Oosterberg het monitoringproject op een zorgvuldige en goede manier af wil ronden	*DAN*	Dienen er in de nazorgfase rollen en verantwoordelijkheden gedefinieerd te worden	*OMDAT*	Dit ervoor zal zorgen dat het project volgens best practices niet zal stranden in de nazorgfase (Modi, 2019)
Types							
OP-04		*ALS*	Oosterberg wil beginnen met het opzetten van monitoring en een startpunt zoekt	*DAN*	Dient er in eerste instantie gekeken te worden naar de monitoring types: "System, Security en ITSM-monitoring"	*OMDAT*	Deze types het beste overeenkomen met de initiële eisen en wensen van de organisatie. Hierna kan er uitbreiding plaatsvinden op basis van business en dependency monitoring
Standaarden							
OP-05	REQ-U-01	*ALS*	Oosterberg de ISO 27001-standaard volgt om logging en monitoring informatie veilig in te richten	*DAN*	Dient artikel A.12.4 (logging en monitoring) gevolgd te worden, dit betreft: - Event logging - Protection of log information - Administrator and operator logs - Clock synchronization	*OMDAT*	Omdat deze vier stappen beschrijven waarom ze van groot belang zijn en omdat op gebied van monitoring op deze wijze voldaan wordt aan de ISO 27001 standaard
OP-06	REQ-B-05	*ALS*	Oosterberg monitoring uit wil breiden in de toekomst	*DAN*	Dient er een Chief information security officer (CISO) aangesteld te worden	*OMDAT*	Dit ervoor zorgt dat de opvolging van regelementen en procedures gegarandeerd wordt, op deze manier gaan er geen belangrijke aspecten van monitoring verloren
OP-07		*ALS*	Oosterberg op herleidbare wijze potentiële incidenten en calamiteiten wil afhandelen	*DAN*	Dient dit gedaan te worden volgens ISO 27001 A.16 (incident afhandeling)	*OMDAT*	Dit garandeert dat het oppakken van incidenten herleidbaar en procesgericht gedaan wordt
OP-08	REQ-B-05	*ALS*	Oosterberg zover is om verder dan het componentniveau te kijken	*DAN*	Kan er volgens ISO/IEC 20000 een Service Management Systeem (SMS) worden opgezet	*OMDAT*	Dit ervoor zorgt dat er op strategische wijze meer gemonitord wordt dan alleen de technologie
OP-09		*ALS*	Oosterberg ICT meer op een lijn met de business wil krijgen	*DAN*	Kan de COBIT-standaard gevolgd worden	*OMDAT*	Deze standaard gespecialiseerd is in het leveren van governance, ten opzichte van ISO
Strategieën							
OP-10		*ALS*	Oosterberg monitoring succesvol op strategische wijze in wil zetten	*DAN*	Dient er een monitoringstrategie opgesteld te worden volgens gestandaardiseerde procedures	*OMDAT*	Data op deze wijze opgehaald, geanalyseerd, voorspeld en gerapporteerd kan worden om zo beschikbaarheid te verhogen
OP-11		*ALS*	Oosterberg proactief wil worden in het beheren van de omgeving	*DAN*	Dient monitoring en logging centraal ingericht te worden	*OMDAT*	Er dan voorkomen wordt dat de ICT-organisatie afhankelijk is van gebruikersmeldingen
OP-12		*ALS*	Oosterberg monitoring op een hoger niveau wil krijgen	*DAN*	Dienen business en ICT op een lijn te zitten, met als uitgangspunt business service performance	*OMDAT*	De organisatie op deze manier op een hoger niveau terecht komt, door het inzichtelijk maken van begrippen en doelen
Protocollen							
OP-13		*ALS*	Oosterberg de integriteit van log data wil bewaken	*DAN*	Dient er gewerkt te worden middels monitoringprotocollen	*OMDAT*	De integriteit van getransporteerde data gewaarborgd wordt door het toepassen van een protocol
OP-14		*ALS*	Oosterberg begint met het monitoren op componentniveau en een protocol wil gaan toepassen	*DAN*	Dient er begonnen te worden met het toepassen van het SNMP-protocol	*OMDAT*	Dit protocol het loggen van belangrijke data van infrastructuurcomponenten toelaat en realiseert

Loggen							
OP-15	REQ-U-03 REQ-U-08	*ALS*	Oosterberg logging wil gaan inzetten ten behoeve van cybersecurity	*DAN*	Dient dit gedaan te worden a.d.h.v. een log retentiebeleid	*OMDAT*	Op deze manier voorkomen wordt dat de log data te groot wordt en aangegeven wordt hoelang welke logs bewaard moeten worden. Dit maakt het mogelijk om forensisch onderzoek uit te kunnen voeren
OP-16		*ALS*	Oosterberg een log retentiebeleid wil opzetten	*DAN*	Dient dit gedaan te worden met belanghebbenden vanuit de business tot aan security- en ICT-management	*OMDAT*	Hierdoor gegarandeerd wordt dat de belangrijkste log data in het beleid staat en er strategisch verantwoord gewerkt wordt
OP-17	REQ-B-05	*ALS*	Oosterberg actie wil ondernemen op basis van kritische incidenten	*DAN*	Dient dit gedaan te worden a.d.h.v. een stappenplan	*OMDAT*	Dit garandeert dat er gestructureerd tewerk gegaan wordt en de genomen stappen hierdoor herleidbaar zijn
OP-18	REQ-B-05	*ALS*	Oosterberg toch actie moet nemen op basis van non-kritische incidenten/ logs	*DAN*	Dient dit gedaan te worden a.d.h.v. een actieplan	*OMDAT*	Dit niet alleen voor registratie van de acties zorgt, maar ook voor gestroomlijnde en tijdsefficiënte procedures zorgt
OP-19		*ALS*	Oosterberg logs moet gaan analyseren	*DAN*	Dient dit middels standaarden gedaan te worden, dit betreft standaarden zoals PCI DSS, NIST 800-137 en ISO/IEC 27002	*OMDAT*	Hierdoor wordt het cybersecurityniveau verhoogd en er wordt aangetoond dat Oosterberg kan voldoen aan standaarden
Technische oplossing							
OP-20	REQ-B-07 REQ-U-01 REQ-U-02 REQ-U-08	*ALS*	Oosterberg op korte termijn log management wil inzetten om het cybersecurityniveau te verhogen	*DAN*	Dient er een Log Management Systeem (LMS) of Syslog Management Systeem ingezet te worden	*OMDAT*	Deze oplossingen ervoor zorgen dat er op goedkope(re) en beheervriendelijke manier een oplossing ingezet kan worden
OP-21	REQ-B-03 REQ-B-04 REQ-B-07 REQ-U-01 REQ-U-04 REQ-U-05 REQ-U-08	*ALS*	Oosterberg op lange termijn log management wil inzetten om het cybersecurityniveau te verhogen	*DAN*	Dient er een SIEM-oplossing ingezet te worden	*OMDAT*	Deze oplossing aansluit bij de eisen en wensen van Oosterberg, door trends en correlaties te kunnen analyseren en alles centraal en geautomatiseerd beschikbaar te stellen. Tevens zorgt een SIEM ervoor dat Oosterberg meer cybersecurityuitbreidingen kan hebben in de toekomst en hier zo op anticipeert
OP-22	REQ-B-05	*ALS*	Oosterberg opvolging wil geven aan het monitoringproject door het niveau van cybersecurity nog verder te verhogen	*DAN*	Dient er een Security Operations Center (SOC) ingezet te worden	*OMDAT*	Een SOC ervoor zorgt dat potentiële beveiligingsproblemen uit de organisatie op menselijk, proces en technologisch niveau gedetecteerd, geanalyseerd, gerapporteerd en voorkomen worden
Rapporteren							
OP-23		*ALS*	Oosterberg rapportages wil ontvangen	*DAN*	Dient er eerst helder te zijn welke data en rapportage er verkregen moet worden, waarna de rapportages ingedeeld worden per categorie en in gewenste situatie tot stand komen in overleg met een CSO, CISO en/ of securityspecialist	*OMDAT*	Hierdoor gegarandeerd wordt dat de juiste data bij de juiste personen komt en dit volgens herleidbare procedures gedaan wordt
Ontwerpfase							
OP-24	REQ-B-06 REQ-B-07 REQ-U-02 REQ-U-07 REQ-S-02 REQ-S-03	*ALS*	Oosterberg SIEM wil inzetten ten behoeve van het beveiligings-volwassenheidsniveau	*DAN*	Dient het geïmplementeerd én beheerd te worden door een (MSSP) partner	*OMDAT*	SIEM hierdoor goed en in volledigheid geïmplementeerd wordt, er geen functionaliteiten ongebruikt blijven, dit best practices volgt en omdat het blijkt dat Oosterberg niet de tijd en benodigde kennis heeft om een SIEM op goede manier te kunnen beheren
OP-25	REQ-U-10	*ALS*	Oosterberg gedrag wil analyseren van gebruikers en wijzigingen van bestanden en accounts wil inzien	*DAN*	Dient User Entity Behavior Analysis gebruikt en geïmplementeerd te worden	*OMDAT*	Dit bij veel SIEM-oplossingen geen standaard functionaliteit is en ingezet kan worden als een extra oplossing of module
OP-26	REQ-B-06 REQ-S-03	*ALS*	Oosterberg de impact op de bestaande omgeving wil reduceren	*DAN*	Dient er een partner ingezet te worden die implementeert en beheert	*OMDAT*	Dit op zowel procesmatig als technisch niveau de complexiteit verminderd en ervoor zorgt dat Oosterberg zelf minder hoeft in te richten

Tabel 10 Conclusie literatuurstudie: Ontwerpprincipes

7 Pakketselectie

De literatuurstudie is gericht op monitoring en hoe Oosterberg ervoor kan zorgen dat monitoring volgens best practices centraal ingericht kan worden. I.v.m. de beschikbare en resterende tijd in het project is er in overleg met Oosterberg vastgesteld dat er meer focus komt te liggen op SIEM en de benodigde processen. Dit komt omdat volgens onderzoek blijkt dat SIEM veel voor Oosterberg kan betekenen. Er is echter nog geen onderzoek gedaan naar de beste SIEM-oplossing en de ontwerpfase is al begonnen. Dit hoofdstuk kan beschouwd worden als een 'na-onderzoek' die bij zal dragen aan de ontwerpfase door te concluderen in een aanbeveling over de beste SIEM-oplossing voor de casus van Oosterberg.

SIEM-oplossing

Ontdekken wat de beste SIEM-oplossing voor Oosterberg is, is wellicht het belangrijkste onderdeel van het project voor Oosterberg. Om dit vast te stellen worden er diverse oplossingen onderzocht en beschreven. Een totale vergelijking vindt vervolgens plaats in een multicriteria analyse, die vervolgens concludeert in een aanbeveling.

De zoektocht naar SIEM-oplossingen wordt ingekaderd door alleen te kijken naar de meest gebruikte en populaire oplossingen, met uitzonderingen op veelbelovende, nieuwe en opkomende oplossingen.

Multicriteria decision analysis:

Om de beste oplossing uit te kiezen wordt de methode 'multicriteria decision analysis' uitgevoerd (MCDA). Het doel van deze analyse is om tot de technische oplossing te komen die het beste bij Oosterberg past, terwijl er rekening wordt gehouden met de eisen en wensen van de organisatie. Dit wordt gedaan door relevantie te verwerken in de criteria. De verschillende criteria worden opgehaald uit de requirements. Het is van belang om te melden dat sommige requirements vanuit Oosterberg (voorbeelden zijn REQ-U-05, 06 en REQ-S-01, 02) standaard functionaliteiten van elke SIEM-oplossing zijn. Toch moet er een MCDA uitgevoerd kunnen worden. Hierdoor zijn de eisen en wensen van Oosterberg verwerkt in de criteria, waarbij overige criteria op basis van algemene/ meest voorkomende SIEM-functionaliteiten zijn toegevoegd. 'Threat intelligence' is hier een voorbeeld van: Alle SIEM-oplossingen hebben deze functionaliteit, maar sommigen hebben hier uitgebreidere mogelijkheden voor. Op deze manier worden SIEM-oplossingen zowel op basis van algemene SIEM-oplossingseisen en de eisen van Oosterberg met elkaar vergeleken. De criteria die een requirement aan zich gebonden hebben staan verwerkt in de tabel met deze requirement.

Relevantie & Calculatie:

Er zijn tien oplossingen bekeken en er zijn 17 criteria opgesteld en deze criteria krijgen een relevantie (weight). De relevantie is vastgesteld a.d.h.v. de eisen en wensen van Oosterberg en goedgekeurd door ICT-Manager en de Infrastructuurbeheerder. Vervolgens kunnen de volgende scores worden toegekend: -3, -2, -1, +1, +2, +3. De totaalscore wordt bepaald door het gewicht * score te berekenen. Hierbij wordt alles in de min geclassificeerd als 0 om zo de berekening accuraat te houden. In de tabel staan deze minwaarden getekend om aan te geven of een criteria compleet niet aanwezig is of omdat het niet aanwezig is met een mogelijkheid om het toch te implementeren of integreren.

Calculaties:

Onderstaande tabel geeft in een overzicht alle nummers en achterliggende waarden weer.

	Requirement	w	AT&T	Mana	LogPo	Splun	IBM	LogTh	Elasti	Micro	McAf	Solar
Real-time monitoring		5%	0,15	0,15	0,15	0,15	0,15	0,15	0,15	0,15	0,15	0,15
Incident response		6%	0,18	0,18	0,18	0,18	0,12	0,18	0	0,18	0,18	0,18
User monitoring		4%	0	0,08	0,12	0,12	0,08	0,08	0	0,04	0,08	0,08
Threat intelligence		6%	0,18	0,18	0,18	0,18	0,18	0,18	0,06	0,18	0,18	0,18
Adv. Analytics & machine learning		5%	0	0	0,15	0,15	0,05	0,15	0,15	0,15	0,15	0,05
Advanced threat detection		6%	0,18	0,06	0,18	0,18	0	0,06	0	0,06	0,18	0,18
Log mangement	REQ-U-01	10%	0,3	0,3	0,3	0,3	0	0,3	0,3	0,3	0,3	0,3
Scalability		2%	0,06	0	0,04	0,07	0	0,06	0,06	0,06	0,04	0,04
UI Intuitivity	REQ-U-02	8%	0,16	0,16	0,24	0,24	0,08	0	0,08	0,08	0,16	0,24
Cloud & On premise	REQ-U-07	6%	0,18	0,18	0,18	0,18	0,18	0,18	0,18	0,06	0,18	0,18
Suppport &Implementation		10%	0,1	0,2	0,2	0,3	0	0,2	0,2	0,2	0,1	0,1
Notification Management system	REQ-U-08	6%	0,06	0,12	0,06	0,18	0,06	0,06	0	0,12	0,06	0,06
Host discovery and recognition	REQ-S-05	5%	0,15	0,15	0,05	0,05	0,1	0	0,1	0	0,05	0,1
User Entity & Behavior Analytics		7%	0,07	0	0,07	0	0,07	0	0	0,14	0,14	0
Security tool integrations	REQ-S-06 & 07	4%	0,08	0	0,08	0,08	0	0,08	0,12	0,08	0,08	0
Automation	REQ-S-04	7%	0,21	0,21	0,21	0,21	0,21	0,07	0,21	0,21	0	0,21
Price	REQ-B-02	3%	0,06	0,03	0,06	0,06	0	0	0,09	0	0	0,09
TOTAL		100%	2,12	2	2,45	2,63	1,28	1,75	1,7	2,01	2,03	2,14

Figuur 23 Calculaties MCDA

Conclusie en toelichting MCDA (zie volgende pagina):

De bedrijfsnamen staan boven in de tabel aangegeven, met hun product in het blauw daaronder. Gewicht (relevantie) is net als bij de calculaties aan de linkerkant aangegeven met daar links naast de criteria. Een uitroepteken geeft aan dat betreffende data niet beschikbaar is en/ of verkregen kon worden. Kosten (price) zijn voor veel oplossingen niet te verkrijgen en lastig te bepalen. Dit komt omdat deze leveranciers het alleen vrijgeven op basis van een quote, maar vaak blijkt dat er in de praktijk geen actie op een verzoek wordt genomen.

		AT&T	ManageEngine	LogPoint	Splunk	IBM	LogRhythm	Elastic Search	Microsoft	McAfee	SolarWinds
	Weight	AlienVault USM Anywhere	Eventlog Analyzer	LogPoint	Splunk Enterprise Security	QRadar SIEM	NextGen SIEM Platform	ELK Stack	Azure Sentinel	Enterprise Security Manager	Security Event Manager
Real-time monitoring	5%	+++	+++	+++	+++	+++	+++	+++	+++	+++	+++
Incident response	6%	+++	+++	+++	+++	++	+++	---	+++	+++	+++
User monitoring	4%	---	++	++	+++	++	++	---	+	++	++
Threat intelligence	6%	+++	+++	+++	+++	+++	+++	+	+++	+++	+++
Adv. analytics & Machine learning	5%	-	---	+++	+++	+	+++	+++	+++	+++	+
Advanced threat detection	6%	+++	+	+++	+++	---	+	---	+	+++	+++
Log management	10%	+++	+++	+++	+++	---	+++	+++	+++	+++	+++
Scalability	2%	+++	-	++	+++	-	+++	++	+++	++	++
UI Intuitivity	8%	++	++	+++	+++	+	-	+	+	++	+++
Cloud & On premise	6%	+++	+++	+++	+++	+++	+++	+++	+	+++	+++
Support & Implementation	10%	+	++	++	+++	-	++	++	++	+	+
Notification management system	6%	+	++	+	+++	+	+	-	++	+	+
Host discovery and recognition	5%	+++	+++	+	+	++	-	++	-	+	++
User Entity & Behavior Analytics	7%	+	---	+	-	+	-	---	++	++	-
Security tool integrations	4%	++	--	++	++	--	++	+++	++	++	-
Automation	7%	+++	+++	+++	+++	+++	+	+++	+++	-	+++
Price	3%	++	+	++	++	---	!	+++	!	!	+++
SCORE = Weight x Rating	100%	2,12	2	2,45	2,63	1,28	1,75	1,7	2,01	2,03	2,14

Figuur 24 MCDA Overzicht en resultaten

In de tabel is te zien dat de hoogst scorende oplossing *Splunk: Enterprise Security* is. De producten van LogPoint en SolarWinds maken samen een top 3. Vanuit deze analyse kan daarmee aanbevolen en geconcludeerd worden dat Splunk als beste de eisen en wensen van Oosterberg kan vervullen. Er zijn een tweetal criteria met een erg hoge relevantie, namelijk: *Een goede support/ implementatiepartner vinden en log management.* Ook gedragsanalyses heeft een hoge relevantie, dit is 'UEBA' (User Entitiy & Behavior Analytics). Dit betreft onder andere het inzien van gedrag van gebruikers, data toegang en account permissie wijzigingen. Uit onderzoek blijkt dat veel SIEM-oplossingen deze functionaliteiten niet standaard hebben en dat veel bedrijven ervoor kiezen om een UEBA-oplossing aan te bieden als een ander/ los pakket. Hoewel Splunk aanbevolen wordt en als beste uit te test komt, heeft de oplossing geen standaard UEBA-functionaliteiten. Dit wordt door Splunk aangeboden als een extra oplossing met integratiemogelijkheden op hun SIEM-oplossing. Ook de oplossing van SolarWinds heeft deze functionaliteit niet en zo leveren zij de UEBA-functionaliteiten aan als extra oplossing/ pakket. Als blijkt dat deze functionaliteiten doorslaggevend zijn voor Oosterberg, dat wordt in dat geval wordt aanbevolen om LogPoint te gebruiken. Een korte toelichting van LogPoint kan gevonden worden in het volgende hoofdstuk. LogPoint levert UEBA in de vorm van een module, bij Splunk is het een compleet andere oplossing/ pakket. Splunk scoort op bijna alle criteria enorm goed en dat is terug te zien in de het pakket. Het is een overzichtelijke SIEM-oplossing waar Oosterberg veel profijt uit kan halen. Splunk heeft diverse betaalmodellen en het zal aan Oosterberg zijn om te bepalen welke methode het beste bij de situatie past. Er kan gekozen worden tussen: Workload Pricing, Entity Pricing en Ingest Pricing (Splunk, 2021). Het is aanbevolen om Splunk te laten implementeren door een partner om zo succes te garanderen. Verspreid over heel Nederland zijn hier mogelijke partners voor en Fox-IT is er hier een van. Uit contact met Fox-IT blijkt dat de oplossing Splunk alleen wordt aangeboden in de vorm van een Managed Security Service Provider (MSSP). Hierbij implementeert Fox-IT de oplossing en nemen zij het beheer bij hun eigen SOC zelf in handen. *"Dit is de toegevoegde waarde van Fox-IT, anders kan het beter direct bij de leverancier afgenomen worden". Dit is bij het uitbesteden van beheer van alle SIEM-oplossingen het geval". "Wij implementeren, beheren, ondersteunen, scannen en melden via onze SOC wat er gaande is in het netwerk van Oosterberg".* (Menten, 2021)

Splunk Enterprise Security voldoet aan de volgende requirements en ontwerpprincipes:
REQ: B-02, B-03, B-04, B-06, U-01, U-02, U-04, U-05, U-06, U-07, U-08, S-01, S-02, U-10, U-11, S-04, S-05.
OP: 01, 04, 11, 19.

Voor en nadelen van een MSSP:

Voordelen	Nadelen
Kostenbesparing ten opzichte van eigen securityspecialisten	Nog steeds een CISO in eigen huis nodig
Brede security expertise beschikbaar	Vertrouwelijkheid: Externe partij toegang geven tot gevoelige data
24/7 customersupport (op basis van een SLA)	Verantwoordelijkheid: Gedetailleerde SLA is een must, denkt de partij verder, nemen ze extra stappen, wat moet er gebeuren bij incidenten vanuit intern en extern, er wordt een andere partij ingezet voor een KPI
Compliance management (MSSP's voldoen aan PCI, AVG, ISO etc.)	
Voldoen aan best practices omtrent monitoring en SIEM	

Tabel 11 Voor- en nadelen MSSP (Ponsioen, 2021)

Het alternatief, LogPoint:
"Bij LogPoint betaal je alleen voor wat je nodig hebt. Dit verschilt van andere SIEM-oplossingen omdat er altijd betaald wordt het gehele pakket en dit vaak te duur is voor de gemiddelde SIEM-afnemer/ gebruiker." (Groot, 2021) LogPoint maakt wel gebruik van UEBA en er wordt aangegeven dat LogPoint zich onderscheid door zich te classificeren als een R&D ontwikkelaar. De oplossing is 'simpel', betaalbaar en beheersbaar en dat is precies het doel wat LogPoint heeft (Groot, 2021). Omdat Oosterberg aangeeft dat kosten geen showstopper zijn, zal Oosterberg zelf de keuze moeten maken voor de uiteindelijke oplossing. Door de betaalmethode van LogPoint (betalen voor het aantal logcomponenten/ sources en niet de hoeveelheid data) wordt er rekening gehouden met de toekomst. *"Data groeit elk jaar met 33%, het is verstandig voor organisaties om hierop in te spelen."* (Groot, 2021)
LogPoint baseert haar licentiemodel op de hoeveelheid log-aanleverende apparaten en doet dit niet op basis van events per seconde of hoeveelheid systemen in het netwerk. Hierbij wordt er rekening gehouden met bijvoorbeeld identieke systemen (werkstations). LogPoint kent ook het 'light' licentiemodel dat toepasbaar is voor werkstations, switches, routers en andere systemen die vrij weinig loginformatie aanleveren vanwege de aard van het systeem. De oplossing kent twee verschillende toepassingen: een SIEM-oplossing en de combinatie van SIEM met UEBA (gedragsanalyse van systemen en gebruikers). Over het algemeen wordt de UEBA-toepassing overwogen nadat een SIEM al aanwezig is. De UEBA-module zorgt ervoor dat systemen en gebruikers onderling en met elkaar vergeleken kunnen worden op basis van gedrag.

LogPoint is te implementeren op een hardware appliance, op software in de vorm van een server of in een VMWare of Cloud-omgeving.

8 Ontwerp

Ontwerpbenadering
De ontwerpfase wordt opgebouwd vanuit de randvoorwaarden, criteria en ontwerpprincipes. Uit de conclusie van de contextanalyse kan opgemerkt worden dat dit heldere en concreet beschreven onderdelen zijn. Hierdoor zijn er weinig onduidelijkheden, waarnaast er ook geen scrum-standups of herhaalde iteraties binnen het project worden uitgevoerd. Door deze redenen wordt er middels de Waterval-methode gewerkt. De ontwerpfase wordt opgesplitst in een functioneel en technisch ontwerp. Dit komt omdat de deelvraag 'wat is de impact op bestaande omgeving' in twee onderdelen kan worden beschreven. Dit betreft 'impact op processen' en 'impact op techniek'.

8.1 Functioneel ontwerp

Het functioneel ontwerp beschrijft welke business processen en assets er van belang zijn, er wordt gekeken naar een logisch ontwerp op basis van de bevindingen in de literatuurstudie en er wordt een architectuurontwerp gemaakt van de toekomstige situatie. Tot slot staan hier ook UML-diagrammen weergegeven om de processtromen aan te geven die toepasselijk zijn op de toekomstige/ gewenste situatie. Het technische ontwerp geeft samen met het functionele ontwerp antwoord op de deelvragen: "Wat is de impact van een oplossing op de omgeving van Oosterberg?" en "Wat is de architectuur van de toekomstige situatie?". In het kader van 'impact' wordt er dit functionele ontwerp antwoord gegeven over wat de impact is op de processen en informatiestromen.
Methoden

- Fieldresearch – semigestructureerde interviews met ICT-manager en Infrastructuurbeheerder
- Deskresearch – onderzoek naar SIEM en het inlezen op documentatie van Oosterberg
- Modelleren – ArchiMate voor de architectuurplaat, UML voor de diagrammen
- Adviseren & concluderen – a.d.h.v. ontwerpprincipes en requirements

Kritieke assets
Het inzichtelijk maken van de primaire businessprocessen van Oosterberg, waarbij er gekeken wordt welke kernsystemen er zijn om deze processen te ondersteunen, zal ervoor zorgen dat er middels een 'Top-down approach' tewerk wordt gegaan. Door dit te doen wordt er middels best practices tewerk gegaan en kan herleidbaar worden aangetoond waarom dergelijke beslissingen of adviezen in deze ontwerpfase worden genomen (Modi, 2019).

Het inzichtelijk maken van deze aspecten wordt gedaan door een vijftal vragen te stellen. De antwoorden op deze vragen zijn middels semigestructureerde interviews verkregen. Zowel ICT-Manager als Infrastructuurbeheerder zijn hiervoor gesproken. De vijftal vragen worden hieronder genoemd, waarna ze verder worden uitgewerkt. Deze vragen zijn opgehaald uit de best practices volgens (Modi, 2019) en opgesteld door gebruik te maken van 'hoe te monitoren' volgens (Boer, 2015).

1. Welke rapportages dienen er ontvangen te worden?
2. Wat zijn de primaire businessprocessen van Oosterberg?
3. Wat zijn de kernsystemen die de businessprocessen draaiend houden en ondersteunen?
4. Welke data dient er gemonitord, gelogd en beveiligd te worden van deze kernsystemen?
5. Welke systemen dienen daadwerkelijk in de monitoring te worden gezet en welke logdata is hier van belang?

[1.] Rapportages

Oosterberg geeft aan in eerste instantie zowel op basis van performance als security rapportages te willen ontvangen. Hierbij ligt de nadruk op rapportages die vreemd gedrag kunnen aantonen en rapportages die aan kunnen tonen welke/ hoeveel data er gebruikt wordt.

- Aantal MB's per gebruikersprofiel (+ gemiddelden, top 10 lijst, sterke plotselinge toenames)
- Aantal MB's per gebruiker OneDrive (+ gemiddelden, top 10 lijst, sterke plotselinge toenames)
- Aantal MB's per gebruiker mailbox (+ gemiddelden, top 10 lijst, sterke plotselinge toenames)

[2.] Business processen

Oosterberg geeft aan een top 3 te kunnen formuleren als het gaat om de primaire businessprocessen. Hierbij wordt ook verteld welke daadwerkelijke processen daar het belangrijkste bij zijn.

1. Logistiek: Het picken van orders vanuit de order intake van verkoop, waarna de order verzonden moet worden. Ook is het inslagen van bestelde orders vanuit inkoop van belang.
2. Verkoop: Het intaken van orders, het managen van orders en het verkopen op zichzelf. Dit wordt gedaan door een koppeling van een klanteigen ERP-systeem met die van Oosterberg, dit wordt gedaan middels verkoopkanalen/ platformsystemen. Daarnaast wordt het ook via de e-mail, telefoon en webshop gedaan.
3. Inkoop: 30% van de producten zijn niet op voorraad dus dient inkoop dit terplekke binnen te halen op het moment dat het aangevraagd wordt. Dit wordt via Triathlon (ERP-systeem) gegenereerd, richting de leverancier gemaild en/ of middels Edi-systemen geregeld. Er wordt gewerkt volgens Edifact standaarden (system2system).

[3.] Kernsystemen, [4.] Log data & [5.] Prioriteiten

Oosterberg geeft aan dat er 13 kernsystemen zijn, waarvan er 8 koste wat het koste dienen te draaien. Deze 8 kernsystemen hebben namelijk geen directe alternatieve vervanging en dienen als primaire methode om de businessprocessen te ondersteunen. Onderstaande lijst is een opsomming van deze systemen en voor welk van de drie businessprocessen ze belangrijk zijn, waarbij ook wordt aangegeven welke data er van deze systemen van belang is en welke kernsystemen daadwerkelijk meegenomen dienen te worden in het ontwerp van de toekomstige situatie. Er is gekeken naar hoe belangrijk de beschikbaarheid, integriteit en vertrouwelijkheid van elk object is. Dit wordt gedaan door de BIV-classificatie aan te houden, deze indeling/ classificatie staat vaak centraal in informatiebeveiliging. Deze BIV-classificatie wordt ingedeeld op basis van persoonlijke gesprekken met de belanghebbenden en wordt uitgevoerd middels een Business Impact Analyse (BIA). De geïdentificeerde informatiesystemen worden door belanghebbenden gewaardeerd t.a.v. benodigde BIV-waarden. Prioriteit wordt bepaald door B*I*V te berekenen. Alle waarderingen met een waarde van 18 of hoger worden meegenomen in de modellen binnen de ontwerpfase. Voor de BIV waarderingen wordt gebruik gemaakt van de volgende waardering index:

Beschikbaarheid	
3	Hoge beschikbaarheid – de dienstverlening mag niet worden verstoord. Bij uitval kans op grote (reputatie) schade.
2	Medium beschikbaarheid – informatie mag slechts gedurende een korte tijd niet beschikbaar zijn. Dit zal beperkte schade opleveren.
1	Lage beschikbaarheid – informatie mag af en toe niet beschikbaar zijn. Uitval leidt tot weinig/ geen schade.
0	N.v.t.
Integriteit	
3	Hoge integriteit – informatie moet gegarandeerd correct zijn. Indien informatie niet correct is, kan dit leiden tot grote schade.
2	Medium integriteit – blijvende juistheid van informatie moet gewaarborgd zijn. Sommige toleranties zijn toelaatbaar.
1	Lage integriteit – indien informatie niet correct is, leidt dit tot weinig of geen schade
0	N.v.t.
Vertrouwelijkheid	
3	Hoge vertrouwelijkheid (Geheim) – informatie is uitsluitend toegankelijk voor een zeer selecte groep personen
2	Medium vertrouwelijkheid (Vertrouwelijk) – er kan substantiële schade zijn indien informatie toegankelijk is voor ongeautoriseerde personen
1	Lage vertrouwelijkheid (Intern) – het openbaar worden van gegevens leidt tot weinig of geen schade
0	Publiek – informatie is openbaar, bestemd voor iedereen

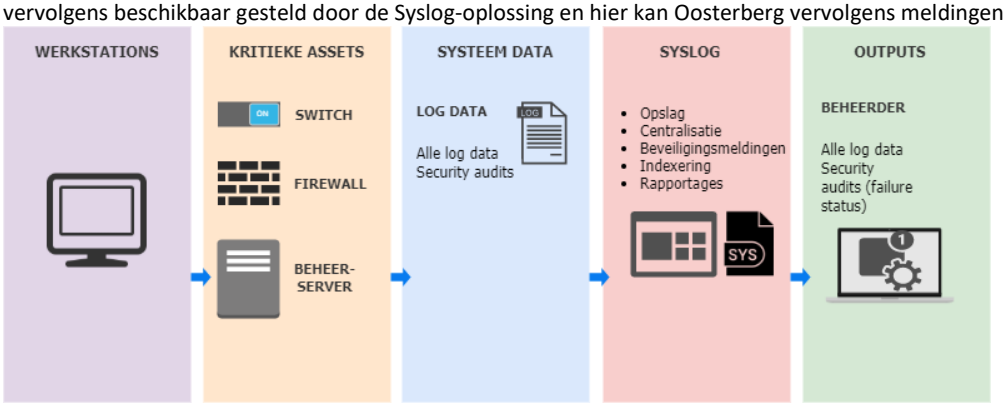
Tabel 12 BIV-waardering index (Ponsioen, 2021)

Nr.	Object	Businessproces	B	I	V	Borging requirements	Waarde
1	Router	Alle 3	**3**	**3**	**3**	REQ-U-09, S-03	27
2	Core switches	Alle 3	**3**	**3**	**3**	REQ-U-09, S-03	27
6	Nimble Storage	Alle 3	**3**	**3**	**3**	REQ-U-09	27
3	Locus	Logistiek	**3**	**3**	2		18
4	Triathlon ERP	Verkoop	2	**3**	**3**		18
5	WLAN-controller	Logistiek	2	**3**	**3**	REQ-U-09	18
7	Desktop Oosterberg	Alle 3	2	**3**	**3**		18
8	Azure o365	Inkoop en verkoop	2	**3**	**3**	REQ-U-07, S-02	18
9	E-Commerce platform	Verkoop	2	**3**	2		12
10	Edge switches	Verkoop	2	**3**	2		12
11	Telefonie	Verkoop	*1*	**3**	2		8
12	EDI Centric DataXchange	Inkoop	*1*	2	*1*		2
13	MessageService	Verkoop	*1*	2	*1*		2

Tabel 13 De kernsystemen van Oosterberg

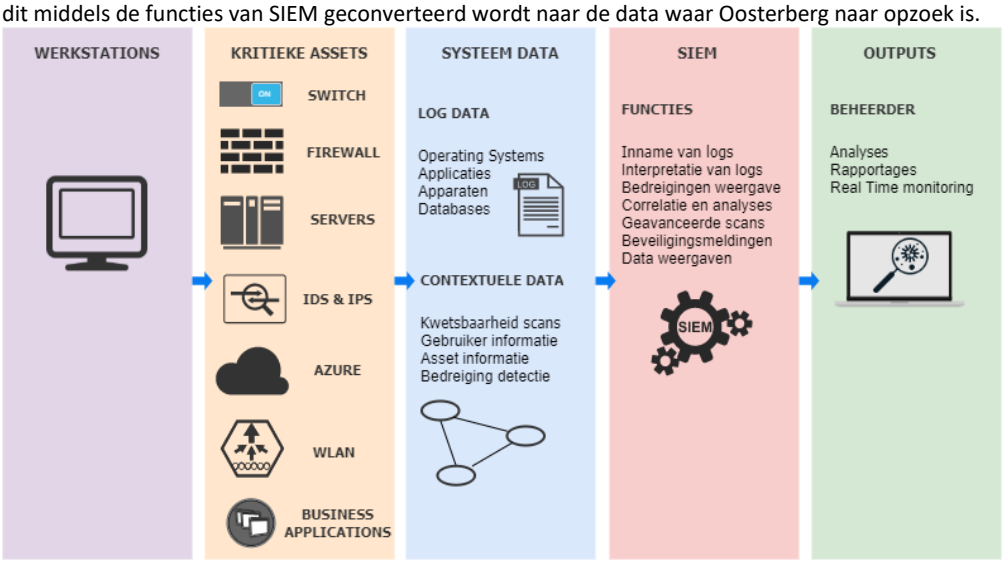
De belangrijkste logdata is te vinden in de bijlage 'functioneel ontwerp – belangrijkste log data'.

Architectuur:
Aanbevelingen en ontwerpen op basis van dit monitoringsproject kan worden gedaan in verschillende dimensies. Vanuit de literatuurstudie zijn er constateringen geformuleerd die onderdelen bevatten zoals standaarden, protocollen, strategieën en technieken. In overleg met Oosterberg is er vastgesteld dat er bij het ontwerpen een focus ligt op een SIEM-oplossing en de belangrijkste onderdelen daaromheen (benodigde processtromen, richtlijnen etc.). Hierbij is het in eerste instantie van belang dat de omgeving van Oosterberg beschermd wordt op mogelijke aanvallen van buiten het netwerk. Op deze manier wordt het ontwerp/ de scope van het project meer ingekaderd en kan er gericht ontworpen worden.
Allereerst wordt er een functioneel architectuurontwerp gemaakt. Bij het ontwerpen is er op basis van best practices en op basis van de kritieke assets begonnen op het componentniveau (de infrastructuur).
Huidige situatie:
Om te beginnen wordt de huidige situatie bekeken. Er staat er een tijdelijke Syslog-oplossing in de omgeving van Oosterberg. Deze Syslog-oplossing haalt tegelijkertijd te veel en weinig data op. De kritieke assets die momenteel in deze logoplossing staan zijn de core-switches, de firewall en de managementserver. Van de eerste twee componenten wordt alle data opgehaald en van de managementserver worden alleen security audits opgehaald met de status 'failure'. Deze data wordt vervolgens beschikbaar gesteld door de Syslog-oplossing en hier kan Oosterberg vervolgens meldingen van ontvangen.



Figuur 25 Ontwerp van huidige situatie van log management bij Oosterberg

Toekomstige situatie:
In de toekomstige situatie zal het geheel er anders uitzien. De Syslog-oplossing wordt vervangen door Splunk SE, waarbij er niet alleen meer kritieke assets in de oplossing worden meegenomen, maar er ook meer data geanalyseerd zal worden. Belangrijke punten zijn de Cloud omgeving Azure en de Intrusion Detection & Prevention Systems (IDS & IPS). Deze bestaan momenteel niet en zijn onderdelen die SIEM oppakt. Daarnaast kan contextuele data inzichtelijk gemaakt worden, waarbij dit middels de functies van SIEM geconverteerd wordt naar de data waar Oosterberg naar opzoek is.



Figuur 26 Ontwerp van toekomstige situatie van log management bij Oosterberg

8.1.1 Deelvraag: Wat is de architectuur van de toekomstige situatie?

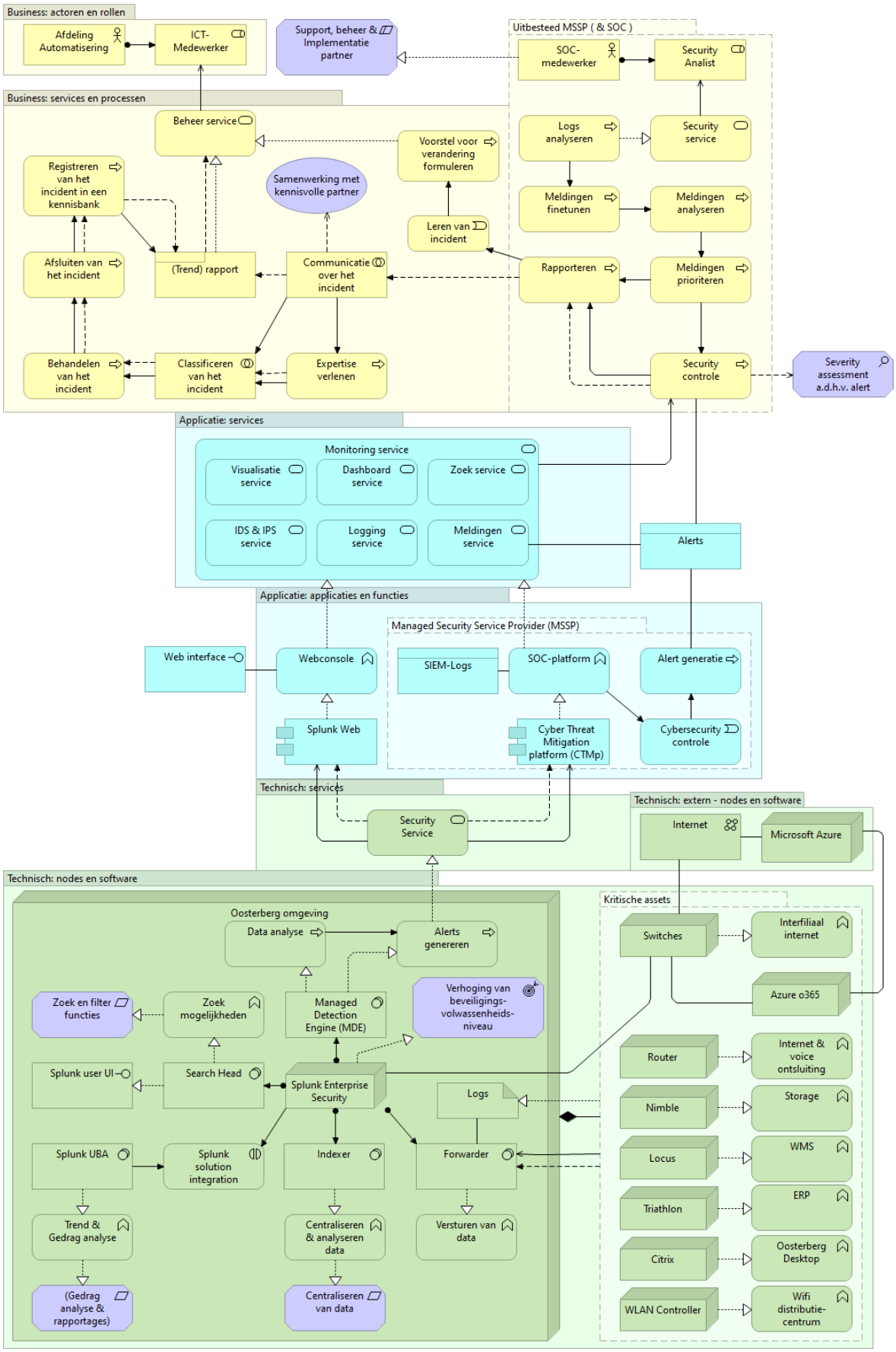
In dit onderdeel wordt de toekomstige situatie gemodelleerd middels ArchiMate. In de contextanalyse is de huidige IST-situatie gemodelleerd, hier wordt de SOLL-situatie gemodelleerd. Drie architecturale lagen zijn aanwezig (business, applicatie en technisch) en worden beschreven per ontwerp en per laag. Na de beschrijvingen wordt aanbevolen welk scenario het beste door Oosterberg gevolgd kan worden.
Er worden een tweetal tekeningen ontworpen *(zie volgende twee pagina's):*

- Ontwerp 1: Alles wordt uitgevoerd door een partner in de vorm van een Managed Security Service Provider (MSSP). Deze implementeert de SIEM-oplossing, neemt het analyseren en detecteren van meldingen in behandeling in hun eigen SOC en lost samen met Oosterberg potentiële incidenten op.
- Ontwerp 2: De implementatie wordt (volgens best practices) uitgevoerd door een partner, maar beheer wordt volledig in eigen huis uitgevoerd door Oosterberg. Veranderingen vinden in dit geval pas plaats op de applicatie en business lagen.

Ontwerp 1: MSSP	Ontwerp 2: Eigen beheer
Business	**Business**
Monitoring dient volgens beschreven processen opgepakt te worden. Dit kan gedaan worden door interne medewerkers of medewerkers van een SOC. Met de hulp van een partner in de vorm van een MSSP wordt dit voor Oosterberg gedaan. Er zal een minimale impact zijn op de bestaande processen, omdat deze monitorings- en incidentprocessen uitgevoerd worden bij het MSSP in hun eigen SOC. Oosterberg hoeft alleen rekening te houden met mogelijke incidenten die opgelost moeten worden, hier zijn de processen voor uitgemodelleerd. Het SOC voert security checks uit en prioriteert meldingen op basis van parameters vanuit Oosterberg. Op het moment dat er een gevonden is, dient er overleg plaats te vinden en dient dit opgepakt te worden.	Bij eigen beheer is er geen bestaande SOC om op terug te vallen en zal Oosterberg zelf het analyseren, prioriteren, rapporteren en oplossen moeten oppakken. In het ontwerp is aangegeven dat het mogelijk is om hier zelf een SOC voor op te richten. Dit is een aanbeveling vanuit het onderzoek middels best practices. Oosterberg zal hier medewerkers voor aan moeten nemen en zal een security specialist in huis moeten halen of moeten trainen om op verantwoorde manier de security aspecten op te pakken en te waarborgen. Ook is Oosterberg in dit geval zelf verantwoordelijk voor het opstellen van een retentiebeleid, voor het opstellen van rapportages en beheren van de applicaties.
Applicatie	**Applicatie**
Door het inzetten van een SIEM-oplossing (Splunk) worden er een aantal applicatie/ monitoringservices centraal ingezet in de organisatie. Al deze services worden door het SOC gebruikt om hun werkzaamheden uit te voeren. De services worden gerealiseerd door het SOC-Platform en Splunk Web. Het SOC-Platform is een functie van het cyber threat mitigation platform 'CTMp', deze applicatie voert geautomatiseerd een cybersecurity controle uit, genereert alerts en stuurt dit in de vorm van een melding door naar SOC-medewerkers voor een handmatige security controle.	Vanuit de technische laag worden dezelfde services ook bij eigen beheer gerealiseerd. Deze monitoringservices zorgen ervoor dat door security specialist en SOC-medewerker data kan worden geanalyseerd. In beide scenario's heeft Splunk een databank om incidenten te managen, maar zal Oosterberg hier zelf beheer op moeten uitvoeren. Hier kan uiteraard ook een third-party oplossing voor worden ingezet. De applicatielaag is verder minder uitgebreid bij deze oplossing, omdat Splunk zich op de technische laag bevindt en er geen geautomatiseerde scan-oplossingen vanuit een MSSP worden gebruikt.
Technisch	**Technisch**
Op de technische laag zijn de kritieke assets en Splunk met alle betreffende componenten gemodelleerd. Vergeleken met eigen beheer zijn hier twee grote verschillen, namelijk het toevoegen van een Managed Detection Engine (MDE) met bijkomende technische processen en het feit dat er geen managed service is. Deze MDE voert automatisch dataanalyses uit en genereert hier alerts uit die door worden gestuurd naar het CTMp. Splunk Enterprise Security heeft een aantal 'core-components'. Dit betreft de forwarder voor het versturen van data van kritieke assets, de indexer om data te centraliseren en analyseren en de search-head die zoek- en filter functionaliteiten realiseert. In de tekening is ook de UBA-oplossing van Splunk gemodelleerd, zo wordt er aangegeven dat de mogelijkheid bestaat om dit te laten integreren.	De technische laag heeft bijna geen verschil vergeleken met het MSSP-ontwerp. De twee grote verschillen zitten in de Managed Detection Engine en de management service. Omdat er geen MDE is, zal dit betekenen dat ook op dit onderdeel Oosterberg zelf data analyses uit zal moeten voeren. Daarnaast bestaat er dus geen uitbesteed beheer en zal Oosterberg zelf Splunk en de mogelijke incidenten moeten managen. Hierdoor wordt de 'mangement service' gemodelleerd. De overige aspecten van de technische laag zijn hetzelfde, omdat Splunk uiteraard op dezelfde onderdelen ingezet moet worden en hiervoor dezelfde componenten gebruikt.
Voldoet aan requirements en ontwerpprincipes	**Voldoet aan requirements en ontwerpprincipes**
OP-01, OP-03, OP-04, OP-11, OP-15, OP-20, OP-21, OP-22, OP-23, OP-24, OP-25, OP-26 *REQ-B-02, REQ-B-03, REQ-B-05, REQ-B-06, REQ-U-01, REQ-U-02, REQ-U-05, REQ-U-06, REQ-U-07, REQ-U-08, REQ-U-09, REQ-S-01, REQ-S-02*	*OP-01, OP-04, OP-20, OP-11, OP-15, OP-20, OP-21* *REQ-B-02, REQ-B-03, REQ-B-06, REQ-U-01, REQ-U-05, REQ-U-06, REQ-U-07, REQ-U-08, REQ-U-09, REQ-S-01, REQ-S-02*
Conclusie/ Aanbeveling	
Uit persoonlijke gesprekken met ICT-Manager blijkt dat Oosterberg een regie ICT-afdeling heeft en momenteel niet over de bezetting en nodige kennis beschikt om een SIEM-oplossing in volledigheid te kunnen beheren. Daarnaast blijkt uit onderzoek naar best practices dat het aanbevolen wordt om niet alleen een SIEM-oplossing te laten implementeren, maar hier ook een Security Specialist, Analyst, CISO en/of een SOC voor te hebben. Momenteel heeft Oosterberg geen van deze rollen of onderdelen in huis en kan daarmee de aanbeveling op volgende wijze worden geformuleerd: • Er wordt aanbevolen om Splunk te laten implementeren door een partner en deze partner vervolgens als MSSP te laten fungeren om Oosterberg accurate en tijdige meldingen te geven middels een platform dat tot in volledigheid kan worden beheerd • Er wordt aanbevolen om de UBA-oplossing van Splunk te integreren nadat de oorspronkelijke oplossing een tijd staat en geconfigureerd is • Er wordt aanbevolen om met deze eerste stap te beginnen, waarna er in de toekomst altijd nog een mogelijkheid bestaat om meer in eigen huis te beheren op het moment dat hier meer kennis en tijd voor is. Het advies wordt hiermee geconcludeert en er kan gesteld worden dat 'Ontwerp 1: MSSP' het beste gevolgd kan worden. *Deze aanbeveling voldoet aan ontwerpprincipes: OP-01, OP-03, OP-04, OP-11, OP-15, OP-20, OP-21, OP-22, OP-23, OP-24, OP-25, OP-26 en requirements: REQ-B-02, REQ-B-03, REQ-B-05, REQ-B-06, REQ-U-01, REQ-U-02, REQ-U-05, REQ-U-06, REQ-U-07, REQ-U-08, REQ-U-09, REQ-S-01, REQ-S-02*	

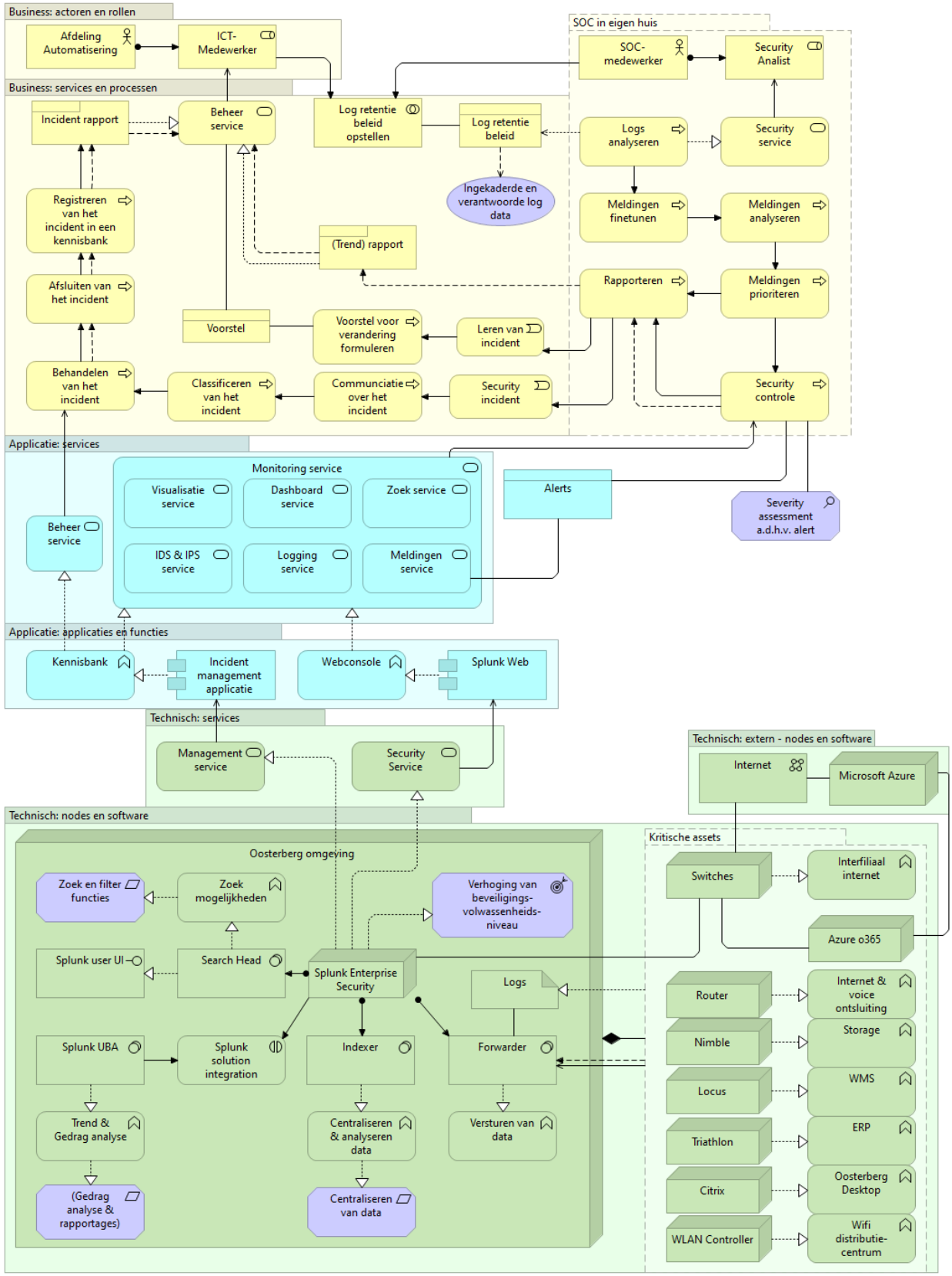
Tabel 14 SOLL-Architectuursituaties

Tekening 1: SIEM gecombineerd met een Managed Security Service Provider (MSSP):



Figuur 27 SOLL Architectuurontwerp - MSSP

Tekening 2: SIEM (laten) implementeren en zelf het beheer in handen nemen:



Figuur 28 SOLL Architectuurontwerp - eigen beheer

8.1.2 Deelvraag: Wat is de impact van een oplossing op de bestaande omgeving? (procesmatig)

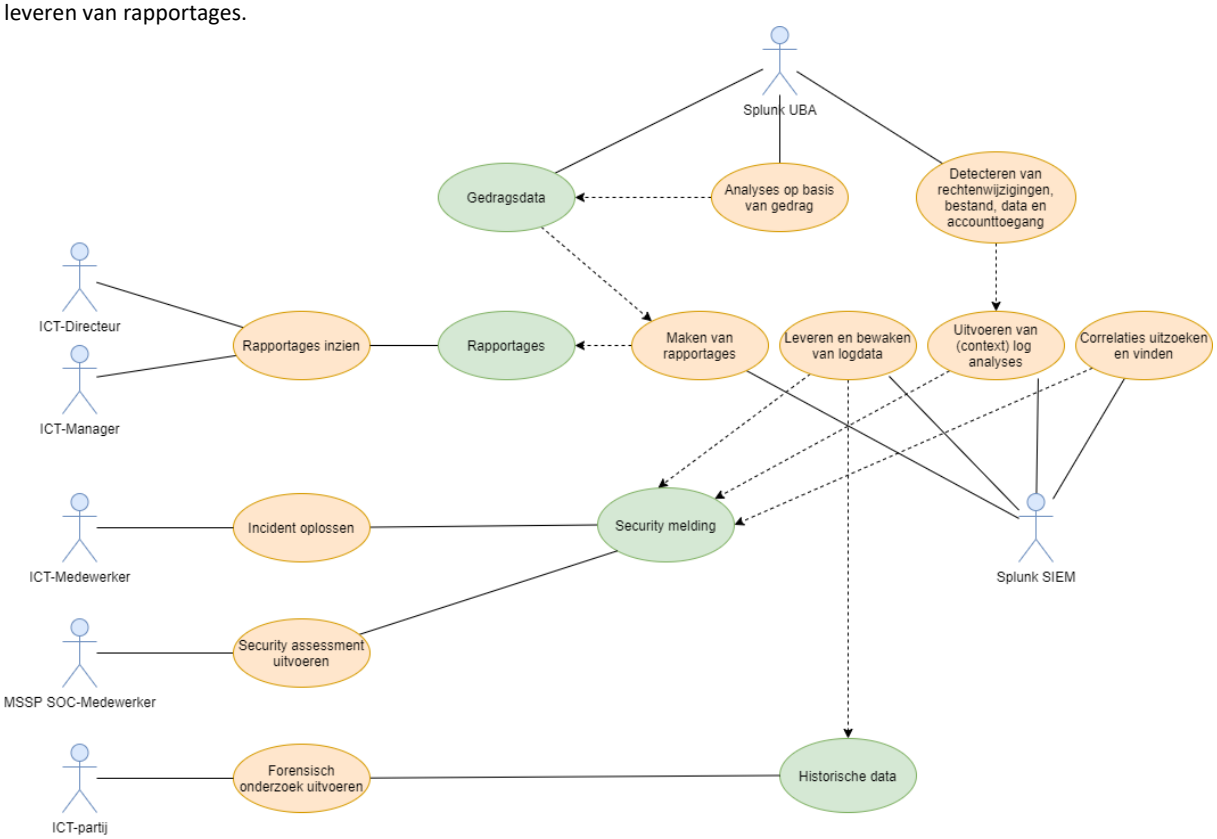
Op basis van de architectuurtekeningen en de onderstaande UML-diagrammen wordt er gekeken naar de impact op de bestaande omgeving. Deze vraag wordt in dit functionele ontwerp ingekaderd door te kijken naar processen en het operationeel beheer dat benodigd is om een oplossing werkend te krijgen en te onderhouden.

Diagrammen:

In dit hoofdstuk worden alle toepasbare (UML) diagrammen ontworpen. Er wordt begonnen met een Usecase-diagram om aan te tonen wat de verschillende manieren zijn waarop een stakeholder in aanraking kan komen met de SIEM-oplossing. Diagrammen worden ontworpen a.d.h.v. SOLL-architectuurtekening 1 (MSSP).

Usecase diagram:

Dit Usecase diagram laat zien dat er nu een forensisch onderzoek uitgevoerd kan worden door een ICT-partij, terwijl dit voorheen niet kon. Ook geeft het diagram aan dat security assessments en werkzaamheden door de MSSP SOC-medewerker worden uitgevoerd. ICT-medewerkers van Oosterberg zijn nog wel betrokken bij het verhelpen en oplossen van mogelijke incidenten. Zowel manager als directeur kunnen rapportages inzien, die aangeleverd worden vanuit de SIEM-oplossing. In dit Usecase diagram is ook Splunk UBA (UEBA) gemodelleerd, waarbij te zien is dat ook deze oplossing kan bijdragen aan het leveren van rapportages.

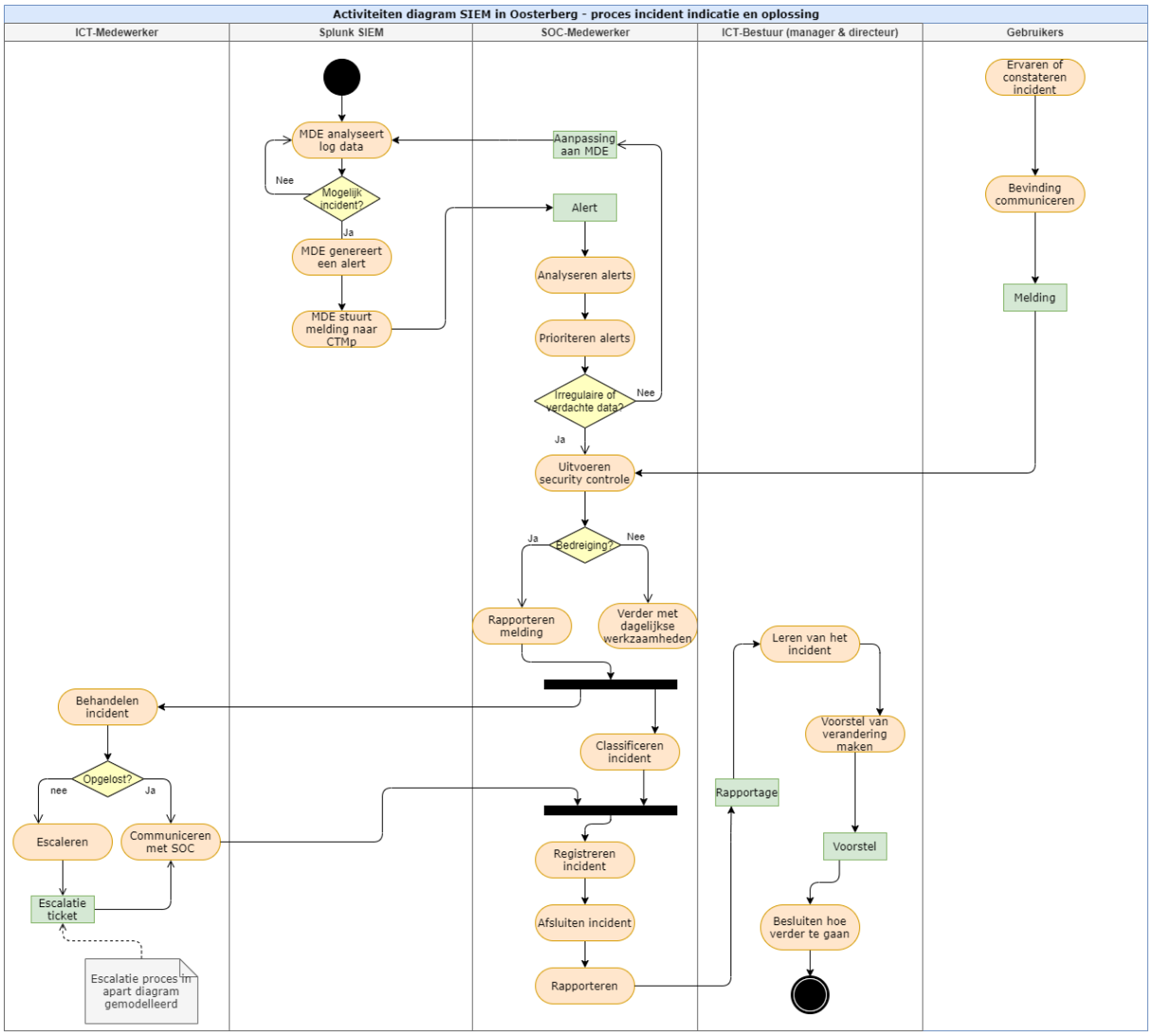


Figuur 29 UML Use Case diagram

Activity diagram:

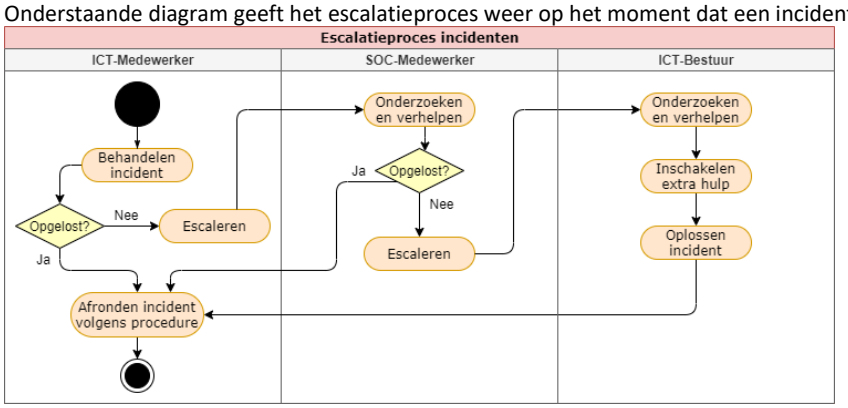
Op de volgende pagina wordt het activiteiten diagram gevisualiseerd en wordt zo het proces omtrent het analyseren en detecteren van mogelijke bedreigingen/ incidenten gemodelleerd. Dit diagram toont daarnaast hoe de meldingen (alerts) worden opgepakt door diverse betrokken stakeholders en wat de processtroom daarbij is. Dit diagram ondersteunt de aanbeveling vanuit de architectuurtekening, omdat ook in dit diagram te zien is dat bijna alle processen geautomatiseerd of uitbesteed kunnen worden. Dit bevestigt de aanbevelingen en resulteert in een minimale impact op de bestaande omgeving van Oosterberg.

Dit draagt bij aan: REQ-S-02, REQ-S-03



Figuur 30 UML Activity diagram – scannen en incidentbeheer

Onderstaande diagram geeft het escalatieproces weer op het moment dat een incident niet opgelost kan worden.



Figuur 31 UML Activity diagram - escaleren

Conclusie deelvraag:

De conclusie wordt gebaseerd op de ArchiMate-modellen en UML-diagrammen. Wanneer er gekeken wordt naar de processen en het beheren van applicaties kan er gesteld worden dat er een minimale impact op de bestaande omgeving zal plaatsvinden. Het uitbesteden van de implementatie en het beheren van de oplossing door een MSSP in te zetten draagt hieraan bij. Dit houdt ook in dat, op het moment dat er gekozen wordt om meer in eigen huis te gaan beheren, er een toename zal zijn aan werkzaamheden, processen, operationeel beheer en mogelijke werkdruk.
De conclusie op de vraag over impact op de techniek wordt beschreven in het technische ontwerp.

Dit draagt bij aan: REQ-S-02, REQ-S-03

8.2 Technisch ontwerp

Inleiding

Het technisch ontwerp beschrijft de technische aspecten van dit project. Dit betreft het uitwerken van de technische onderdelen en implementatie van Splunk Enterprise Security, hoe de data binnen de componenten zal stromen en het technische ontwerp geeft samen met het functionele ontwerp antwoord op de deelvragen: “Wat is de impact van een oplossing op de omgeving van Oosterberg?” en “Wat is de architectuur van de toekomstige situatie?”. In het kader van ‘impact’ wordt er in het technisch ontwerp antwoord gegeven op technische performance door een architectuurontwerp te maken.

Technische requirements & Implementatie:

Om de architectuur en infrastructuur te kunnen ontwerpen wordt de aanname gedaan dat Splunk verder meegenomen zal worden binnen Oosterberg. Op het moment dat dit niet zo is, heeft dit minimale gevolgen voor de architectuurmodellen.
Splunk kan op drie wijzen worden geïmplementeerd: Single instance deployment, Distributed search deployment en in Splunk Cloud. Het is van belang dat helder is wat deze verschillende deployments betekenen:

Single instance:

Dit is een standalone instance die zowel het indexeren als het zoeken uitvoert. Hier dient er ingelogd te worden op Splunk Web of de CLI op de instance om data input te configureren, om zo data te kunnen verzamelen. Deze machine wordt daarna dus ook ingezet om data te verzamelen, monitoren melden en rapporteren.

Distributed:

Om de load van de server te verminderen kan een distributed deployment worden ingezet. Dit kan worden gedaan door meerdere ‘indexers’ en load balancers op te zetten. De functies van een single instance worden als het ware zo meer verspreid. Dit houdt in dat er dus ook gespecialiseerde instances in het netwerk komen te staan.

Cloud deployment:

Splunk Enterprise Security is ook beschikbaar als service in Splunk Cloud. Deze Cloud architectuur verschilt op basis van data en het aantal zoekopdrachten die uitgevoerd worden. Splunk Cloud is een service gebaseerd op een abonnement en kan afgenomen worden op basis van een contract.

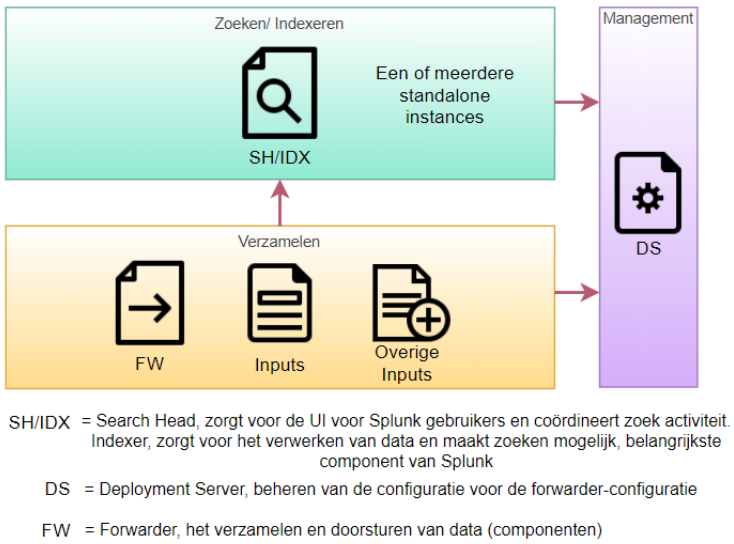
Een overzicht van deze instances/ componenten is te vinden in de onderstaande tabel:

Functies	Indexer	Search Head	Forwarder	Deployment Server
Indexing	x			
Web		x		
Direct search		x		
Forward to indexer			x	
Deploy configurations	x		x	x

Tabel 15 Overzicht van functies (Splunk, 2021)

Infrastructuur/ Splunk-component tekening:

Om aan te tonen hoe de Splunk-componenten werken en waar ze voor dienen, wordt het onderstaande ontwerp gemaakt en getoond:



Figuur 32 Splunk-component tekening

Om te bepalen welke deployment het beste ingezet kan worden voor Oosterberg, levert Splunk een 'Daily indexing volume' tabel aan. Deze tabel geeft weer wat er benodigd is, kortom: Meer gebruikers = meer search heads en meer data = meer indexers.

Daily Indexing Volume						
	<2GB/day	**2 to 300 GB/day**	**300 to 600 GB/day**	**600GB to 1TB/day**	**1 to 2TB/day**	**2 to 3TB/day**
Total Users: less than 4	1 combined instance	1 combined instance	1 Search Head, 2 Indexers	1 Search Head, 3 Indexers	1 Search Head, 7 Indexers	1 Search Head, 10 Indexers
Total Users: up to 8	1 combined instance	1 Search Head, 1 Indexers	1 Search Head, 2 Indexers	1 Search Head, 3 Indexers	1 Search Head, 8 Indexers	1 Search Head, 12 Indexers
Total Users: up to 16	1 Search Head, 1 Indexers	1 Search Head, 1 Indexers	1 Search Head, 3 Indexers	2 Search Head, 4 Indexers	2 Search Head, 10 Indexers	2 Search Head, 15 Indexers
Total Users: up to 24	1 Search Head, 1 Indexers	1 Search Head, 2 Indexers	2 Search Head, 3 Indexers	2 Search Head, 6 Indexers	1 Search Head, 12 Indexers	3 Search Head, 18 Indexers
Total Users: Up to 48	1 Search Head, 2 Indexers	1 Search Head, 2 Indexers	2 Search Head, 4 Indexers	2 Search Head, 7 Indexers	13 Search Head, 14 Indexers	3 Search Head, 21 Indexers

Tabel 16 Samenvatting van performance aanbevelingen (Splunk, 2021)

In verband met de eisen en wensen van Oosterberg kan er gesteld worden dat een single instance deployment zal voldoen. Voor een accurate bepaling dient er contact opgenomen te worden met Splunk en zal Oosterberg eerst moeten berekenen hoeveel data er opgeslagen en verstuurd zal gaan worden.

Requirements voor een single instance:

Oosterberg mag zelf bepalen op welk operating system Splunk Enterprise Security geïnstalleerd moet worden. Er wordt onderscheid gemaakt tussen keuzes op basis van UNIX en Windows operating systems. Er wordt aanbevolen om Splunk op een dedicated machine te installeren. Op het moment dat Splunk Enterprise Security binnen een virtuele machine draait, zal performance hieronder lijden. Dit komt omdat Splunk ES veel resources nodig heeft om het werk goed te kunnen doen en deze resources moet delen met de VM als het hierop geïnstalleerd wordt. Het wordt aangeraden om Block level storage te gebruiken, ten opzichte van File level storage voor het indexeren van data i.v.m. performance (kortom: gebruik een SAN en geen NAS/ NFS). Hierbij wordt gebruik van een SSD geadviseerd. Overige hardware requirements aan een single instance deployment zijn (Splunk, 2021):

- Een x86 of 64-bit chip architectuur
- 12 fysieke CPU cores of 24 vCPU's op ten minste 2Ghz of hoger
- 12 GB RAM
- 1Gb Ethernet NIC met een tweede optionele voor een managementnetwerk (i.v.m. segmentatie)
- 64-bit Linux of Windows distributie

Dit voldoet aan: REQ-S-01, REQ-S-02

Alarm management:

Splunk Enterprise Security heeft een eigen management interface om de incidenten inzichtelijk te maken. Om Splunk Enterprise Security meldingen te laten versturen naar een tweede (inzage) punt, kan er gebruikt worden gemaakt van e-mail functionaliteiten. Op deze manier kan Oosterberg ervoor zorgen dat mails in TopDesk automatisch worden geregistreerd als incident. Hiervoor zijn alleen een e-mailadres en eventueel een gebruikersnaam en wachtwoord nodig. Verder zal alleen het onderwerp en de prioriteit aangegeven moeten worden. Splunk ES maakt het mogelijk om deze mails en mailinhoud aan te passen. Op deze manier wordt er ingespeeld op de benodigde informatie voor procesmatig werk. Hiervoor kan gerefereerd worden naar onderstaande tabel:

Optie	**Voegt toe aan email**
Link naar Alert (of) Link naar Rapportage	Een link naar de melding of geplande rapport
Link naar Resultaat	Een link naar het resultaat voor de gerelateerde zoekopdracht
Zoekreeks	Een zoekreeks (Search String) die gebruikt wordt door de melding of het rapport
Inline …	Laat het resultaat zien in een tabel in de mail
Trigger conditie	Laat de conditie zien die de melding liet afgaan
Trigger tijd	Laat de tijd zien waarop de melding zich voor doet
Toevoegen van CSV	Het toevoegen van een CSV met de resultaten
Toevoegen van PDF	Het toevoegen van een PDF met de resultaten
Toevoegen lege bijlage	Het toevoegen van een CSV of PDF, zelfs wanneer het resultaat leeg is

Tabel 17 Mail wijzigingsmogelijkheden (Splunk, 2021)

Dit voldoet aan: REQ-S-07

Priority Assessment:
Prioriteiten (severity scores) worden in Splunk Enterprise Security bepaald door de 'urgency_lookup'. Deze functie gebruikt de severity en prioriteit-waarden die toegekend zijn aan een event dat gegenereerd wordt. Events kunnen een aantal waarden toegekend krijgen. Onderstaande tabel toont welke matrix Splunk SE hanteert voor deze berekening. *Dit voldoet aan: REQ-U-11*

Assigned Severity

Assigned Priority	Informational	Unknown	Low	Medium	High	Critical
Unknown	Informational	Low	Low	Low	Medium	High
Low	Informational	Low	Low	Low	Medium	High
Medium	Informational	Low	Low	Medium	High	Critical
High	Informational	Medium	Medium	Medium	High	Critical
Critical	Informational	Medium	Medium	High	Critical	Critical

Tabel 18 Severity scores

8.2.1 Deelvraag: Wat is de impact van een oplossing op de bestaande omgeving? (technisch)

Het implementeren van een SIEM-oplossing in de organisatie heeft impact op zowel processen als de technische infrastructuur. Echter blijkt dat de technische impact alleen plaatsvindt op de machine/ instance waar de SIEM-oplossing zelf op draait. Deze machine zal veel CPU, RAM en data throughput hebben. De componenten die data versturen naar de SIEM hebben verder geen last en impact van de SIEM-oplossing. Dit blijkt uit een interview met een vertegenwoordiger van LogPoint. *"Opgehaalde en te verwerken data van een SIEM-oplossing heeft de minimaalste impact op de bestaande infrastructuur. Dit komt omdat het maar een paar bitjes (eentjes en nulletjes) zijn die verwerkt moeten worden, alle rekenkracht vindt plaats op de machine waar de SIEM-oplossing staat. Dus zowel bandbreedte als CPU-performance en overige aspecten van de bestaande infrastructuur lijden niet onder het toevoegen van een SIEM aan de omgeving".* (Groot, 2021)
Deze bevinding wordt bevestigd door Splunk, waaraan wordt gegeven dat het een minimale of zelfs niet-bestaande impact is. Dit komt omdat SIEM-oplossingen alleen data verwerken die al beschikbaar is of beschikbaar wordt gesteld. Er wordt geen nieuwe data opgewekt uit de componenten (Splunk, 2021).
Dit voldoet aan: REQ-S-03

Ontwerp evaluatie
Het technisch ontwerp wordt afgerond door te testen of de aanbevelingen en ontwerpen deugen. Normaliter wordt hier een prototype voor gemaakt om dit aan te tonen. In dit geval zijn de aanbevelingen dat de implementatie en het beheer worden uitbesteed. Om toch aan te tonen dat de aanbevelingen deugen en haalbaar zijn, wordt er een expert gecontacteerd. Deze expert kijkt de modellen, methodieken en aanbevelingen na en kijkt of de requirements haalbaar zijn met deze onderdelen.
De expert is Managing Director Mitchel Ponsioen van het ICT-bedrijf Wazda en loopt samen met de onderzoeker de beschreven punten langs. Onderstaande opmerkingen en bevindingen zijn genomen tijdens dit assessment:
Algemene indruk:
De algemene indruk over het project is erg goed. Het assessment heeft ongeveer 3.5 uur geduurd en in deze tijd zijn de besproken onderdelen nagelezen en bekeken. Hierbij heeft de onderzoeker toelichtingen gegeven waar nodig. Er wordt aangegeven dat er goed onderbouwd wordt en dat de getrokken conclusies goed doordacht zijn. Gedurende het assessment zijn er algemene aandachtspunten gegeven over de gehele scriptie, waarbij een paar punten wat meer aandacht verdienen. Over de gehele scriptie staat op moment van deze assessment nergens echt goed beschreven hoe er geleerd wordt van incidenten. Er staat wel hoe ze opgepakt dienen te worden, maar niet hoe er vervolgens geleerd van kan worden. Daarnaast verdienen het onderzoek naar kritieke assets van Oosterberg en het model van de SOLL-situatie op basis van een MSSP meer aandacht. Hier dient beter gemodelleerd hoe de processen te scheiden zijn van elkaar en dienen de BIV-waarden beter herleidbaar te worden (Ponsioen, 2021).
Modellen:
Alle ontworpen modellen zijn tijdens dit assessment geanalyseerd. Hierbij kunnen de volgende punten genoteerd worden, waarbij de volgorde van de scriptie wordt aangehouden (zie figuuropgave).

- Incidentflow (onderzoeksrapport)
  - Communicatie op basis van incidenten, hoe te escaleren, communicatie via directie
  - Verbeterproces en communicatie bij ISO-incidenten toevoegen indien tijd dit schikt
  - Procesflow op basis van incident & gebeurtenis kan wellicht toegevoegd worden
- Kritieke assets (functioneel ontwerp)
  - Wellicht kan hier een risicoanalyse/ heat map in worden verwerkt. Zo kan er aangetoond worden waarom de waarden worden toegekend en krijg je meer dan een 'ja/ nee' bij prioriteit
  - Er kan nog onderzocht of beschreven worden waarom er wel of geen actie ondernomen dient te worden bij deze onderdelen. Hier kan een meetmethodiek voor worden ingezet, zoals een BIA (Business Impact Analyse)
  - In deze tabel kan ook worden verwerkt welke requirements onder deze business assets vallen. Dus welke behoeften worden geborgd in de oplossing d.m.v. de kritische systemen
- SOLL-architectuur (functioneel ontwerp)
  - Er wordt aanbevolen om ook de negatieve aspecten van een MSSP te onderzoeken. Dit kan indien mogelijk kort verwerkt worden in de vergelijkingstabel

- Denk na en verwerk wellicht deze punten daarbij: het verantwoordelijkheidsbesef is belangrijk, deze licht nu verspreid intern en extern. De verantwoordelijkheid voor daadwerkelijke uitwerking, er wordt nu een andere partij ingezet voor een KPI
- Hoe dient meedenken en werken te worden opgepakt? SLA, KPI 24/7?
- Hoe diepgaand dient de hulp te gaan – kijk naar kennis, kwaliteit, service
- MSSP-architectuur: SOC beter opsplitsen
- Eigen architectuur: Het leren van de incidenten is nog niet gemodelleerd
- Wat wordt er behaald per ontwerp? – mogelijk verwerken in vergelijkingstabel

Overig

- Splunk referentiecase of use cases toevoegen of beschrijven
- Vervolgstappen in kaart brengen indien de tijd dit schikt

Requirements

Onderstaande requirement-tabel toont aan welke eisen behaald zijn en noteert hier eventuele opmerkingen vanuit het assessment met de expert:

ID	Requirement	Behaald	Opmerking
	Must have requirements		
REQ-B-01	De kosten van een oplossing dienen goed overeen te komen met de baten, maar kosten zijn geen showstopper	Nee	Geen kosten baten Geen directe baten, welke kostenbesparing maak je door redundante tooling (mogelijke uitbreiding)?
REQ-B-02	Er dienen (trend)rapportages opgehaald te kunnen worden, dit betreft rapportages zoals het inzien van toename aan data in gebruiker mail, profiel en OneDrive	Ja	Theoretisch
REQ-B-03	Er dienen analyses uitgevoerd te kunnen worden op basis van trends en afwijkingen in deze trends, dit betreft trends zoals het inzien van toename aan data in gebruiker mail, profiel en OneDrive	Ja	Theoretisch
REQ-B-04	Vervolgstappen a.d.h.v. dit project dienen inzichtelijk gemaakt te worden	50/50	Valt buiten scope, in de vorm van aanbevelingen sturing gegeven
REQ-B-05	Gebruikersondersteuning dient snel aangevraagd te kunnen worden, waarbij de organisatie geholpen wordt door een partner door support en wellicht bij implementatie en/ of beheer	Ja	SLA goed overwegen na dit project
REQ-B-06	Bedrijfscontinuïteit dient bewaakt te worden door de verhoging van het beveiligingsniveau, waarbij op lange termijn het tactische niveau behaald dient te worden en op korte termijn het proactieve (volwassenheid)niveau	Ja	
REQ-B-07	Het inrichten van mogelijke KPI's voor ICT dient bestudeert te worden	Ja	
REQ-U-01	Log data dient compacter, meer gecentraliseerd en informatiever gemaakt te worden	ja	
REQ-U-02	De oplossing dient gebruik- en beheers vriendelijk te zijn, het mag niet te complex worden en dient daarom intuïtief te werken en/ of in te spelen op bestaande werkzaamheden. Dit zal moeten blijken uit mogelijke reviews van een oplossing	Ja (50/50)	Complexe materie, outsourcing, niet te behalen
REQ-U-03	Er dient duidelijk te worden gemaakt welke logs hoelang en waar bewaard moeten worden	Ja	
REQ-U-04	Er dient inzichtelijk te worden gemaakt wat best practices omtrent monitoring zijn	Ja	
REQ-U-05	De oplossing dient een voorziening te hebben om te kunnen filteren en zoeken	Ja	
REQ-U-06	De oplossing dient eventherkenning te hebben om te zien welke events wanneer voor komen	Ja	
REQ-U-07	De oplossing dient zowel on premise als in de Cloud (Azure) logs op te kunnen halen	Ja	
REQ-U-08	De oplossing dient een ingebouwd managementsysteem te hebben om meldingen goed te kunnen keuren	Ja	
REQ-U-09	Historische data dient beschikbaar te worden gemaakt voor forensisch onderzoek	Ja	
REQ-S-01	De oplossing dient voor zover mogelijk gescheden te zijn van de bestaande infrastructuur i.v.m. veiligheid en beschikbaarheid	Ja	
REQ-S-02	De oplossing dient te integreren te zijn met de huidige infrastructuur en omgeving	Ja	
REQ-S-03	Er dient aangetoond te worden wat de impact op systeemperformance is van een oplossing. Een oplossing mag de systemen niet traag maken	Ja	Extra bevestiging door Referentiecase (use case?)
	Should have requirements		
REQ-U-10	De oplossing moet aantonen dat er een hacker is en welke rechten deze hacker heeft verkregen	Ja	
REQ-U-11	De oplossing dient 'severity scores' te kunnen hangen aan events die meer prioriteit verdienen om zaken te kunnen managen en overzichtelijk te houden	Ja	
REQ-S-04	De oplossing moet kunnen automatiseren d.m.v. het gebruik van templates	Ja	
REQ-S-05	De oplossing dient systeemherkenning te hebben op basis van type of merk. De oplossing dient veel intelligentie met de oplossing mee te komen, waardoor beheer en inrichting eenvoudig worden gemaakt	50/50	Ja, maar geen specifiek onderzoek naar pakketten van oosterberg, maar kan vervolgd worden
REQ-S-06	Oosterberg wil graag weten of het mogelijk is om meer applicaties te loggen of te integreren. Integratiemogelijkheden omtrent o365 zijn van belang	Ja	
	Could have requirements		
REQ-S-07	De oplossing dient geïntegreerd te kunnen worden met TopDesk of dient zelf 'tickets' te managen	Ja	
	Won't have now		
REQ-B-08	Het inrichten van KPI's dient voor ICT gerealiseerd te worden	Ja	Partner voor aanstellen
REQ-B-09	Het opstellen van een logretentiebeleid dient gerealiseerd te worden	Ja	
REQ-U-12	Het inrichten van een documentatie managementsysteem dient gerealiseerd te worden	Nee	Niet behandeld

Tabel 19 Requirement controle met Expert

9 Eindevaluatie

Inleiding

In dit hoofdstuk worden de scriptie en het gehele afstudeertraject afgerond. Het onderzoek wordt geconcludeerd in een korte beschrijving van het probleem, gevolgd door de resultaten van alle deelvragen en de hoofdvraag. Tot slot wordt er een waardeoordeel uitgesproken over het ontwerp en het ontwerponderzoek, waarbij dit afgerond wordt met een advies aan Oosterberg.

Het probleem

Oosterberg ziet graag verbeteringen op gebied van cyber security, door het beter beheren van logs en het toepassen van monitoring en analyse. Forensisch onderzoek kan momenteel niet volledig uitgevoerd worden door een gebrek aan historische data, tijdige constateringen omtrent beveiligingslekken en het kunnen uitvoeren van analyses. Dit komt gedeeltelijk omdat Oosterberg zich momenteel begeeft in een reactieve ICT-omgeving. Oosterberg zoekt naar een advies over hoe een monitoringoplossing ervoor kan zorgen dat bovenstaand genoemde onderdelen opgelost kunnen worden. De organisatie wil op een hoger beveiligings-volwassenheidsniveau komen door monitoring in te zetten. Oosterberg wil graag adviezen over zo'n oplossing en op welke wijze dit het beste geïmplementeerd en geconfigureerd kan worden. Daarnaast wil Oosterberg graag weten hoe het beheerd dient te worden en hoe er procesmatig gehandeld kan worden op signaleringen vanuit het systeem.

Deelvragen

Dit project is gestart met de volgende deelvragen:

- Wat zijn de knelpunten in de huidige situatie?
- Wat is de architectuur van de huidige situatie?
- Wat zijn de eisen die Oosterberg stelt?
- Welke mogelijke conceptuele oplossingen zijn er?
- Wat is de impact van een oplossing op de bestaande omgeving?
- Wat is de architectuur van de toekomstige situatie?

Deze deelvragen beantwoorden de hoofdvraag:

- *"Hoe kan Koninklijke Oosterberg B.V. het monitoren optimaal en centraal inrichten?"*

De Resultaten

Dit hoofdstuk beantwoord de deelvragen die in bovenstaande onderdeel zijn geformuleerd.

- Wat zijn de knelpunten in de huidige situatie?
  De knelpunten in de huidige situatie worden in kaart gebracht door de probleemanalyse. De probleemanalyse staat in het onderzoeksrapport. Uit deze analyse komen vanuit vier perspectieven verschillende problemen en oorzaken boven water. De perspectieven komen voort uit de behoefteanalyse. Kortom blijkt dat Oosterberg geen forensisch onderzoek kan uitvoeren en reactief beheer uitvoert op de omgeving. Ook bestaan er geen processen omtrent monitoring en/ of beheer en zijn er onduidelijkheden omtrent logging, KPI's en conceptuele mogelijkheden om deze problematiek op te pakken.
- Wat is de architectuur van de huidige situatie?
  De architectuur van de huidige situatie wordt in kaart gebracht door de contextanalyse. Deze analyse staat in het vooronderzoek in het onderzoeksrapport. Hier wordt d.m.v. aggregatieniveaus gekeken naar de context van de organisatieomgeving. Het architectuurontwerp is gemaakt op basis van alle belangrijke aspecten die uit interviews verkregen zijn. Er bestaat een logging-tool, hoewel deze op minimale wijze wordt gebruikt. Ook bestaat de monitoringoplossing PRTG en is Oosterberg druk bezig om deze te optimaliseren.
- Wat zijn de eisen die Oosterberg stelt?
  De eisen komen voort uit de perspectieven die middels een stakeholderanalyse in de behoefteanalyse zijn verkregen. Deze behoefteanalyse staat in het vooronderzoek in het onderzoeksrapport. Kort samengevat wil Oosterberg graag dat er een technische oplossing komt om monitoring (met een focus op logging) gecentraliseerd in te zetten. Hierbij moet er volgens best practices gewerkt kunnen worden en wil Oosterberg graag weten hoe de oplossing geïntegreerd kan worden in de organisatie. Daarbij is het van belang dat er inzichtelijk wordt gemaakt wat de impact op business en techniek is.
- Welke mogelijke conceptuele oplossingen zijn er?
  Deze deelvraag is beantwoord in de literatuurstudie in het onderzoeksrapport. Ook de pakketselectie die in de ontwerpfase is uitgevoerd heeft bijgedragen aan deze deelvraag. Monitoring kent veel concepten die in de literatuurstudie zijn toegelicht. Dit betreft best practices, standaarden, strategieën, protocollen, loggen, incidenten, analyseren, monitoren en technische oplossingen. Al deze onderdelen kunnen ingezet worden om Oosterberg monitoring goed te laten inrichten. I.v.m. de eisen en wensen van Oosterberg kan er gesteld worden dat het toepassen van een SIEM-oplossing, het inrichten van een SOC en het volgen van best practices het belangrijkste zijn. Hierbij sluit Splunk Enterprise Security het beste aan bij de eisen van Oosterberg en is het tot slot van groot belang dat er monitoring en incidentprocessen worden gevormd en gevolgd in de organisatie.

- Wat is de impact van een oplossing op de bestaande omgeving?
  Deze deelvraag wordt beantwoord in het functionele en technische rapport. Zowel op proces als technisch niveau kan er impact voor komen. De impact op processen is groter als Oosterberg ervoor kiest om de oplossing in eigen beheer te nemen. De aanbeveling hierbij is om het uitbesteden omdat de processen dan bij de partner plaatsvinden. De impact op techniek is nihil, dit blijkt uit contact met vertegenwoordigers van LogPoint en Splunk. Dit komt omdat SIEM-oplossingen alleen bestaande data gebruiken om informatie te vergaren. Ook informatie die niet eerder gebruikt werd en nu opgewekt wordt heeft bijna geen impact op de omgeving. Impact kan ontstaan als SIEM op een gedeelde server geïmplementeerd wordt. Dit kan worden opgevangen omdat het aanbevolen wordt om dit te scheiden. Hierdoor ondervinden SIEM en de omgeving van Oosterberg de minste performance impact.
- Wat is de architectuur van de toekomstige situatie?
  De architectuur van de toekomstige situatie wordt gemodelleerd in het functionele ontwerp. Hier worden twee scenario's gemodelleerd: Eigen beheer en het uitbesteden van SIEM en beheer. Op deze manier wordt er aanbevolen welk scenario het beste gevolgd kan worden en wordt er een alternatief aangeleverd. Aanbevelingen en conclusies worden getest door de expert in de conclusie van het technisch ontwerp.

Beantwoorden van de hoofdvraag:

In dit onderdeel wordt er antwoord gegeven op de hoofdvraag:

- *"Hoe kan Koninklijke Oosterberg B.V. het monitoren optimaal en centraal inrichten?"*

De onderzoeker heeft dit onderzoeksproject zo breed mogelijk opgestart. Hierbij zijn alle mogelijke concepten beschreven en kunnen deze concepten ingezet worden om monitoring optimaal in te richten. In de context van 'optimaal' wordt er gesproken over best practices en op de wijze waarop monitoring geïntegreerd wordt in de organisatie. Het moet namelijk aansluiten bij de werkfilosofie en werkomgeving van Oosterberg.
Oosterberg kan op een hoger beveiligingsvolwassenheidsniveau komen door een SIEM-oplossing in te zetten. Hiervoor kan Splunk Enterprise Security worden gebruikt. Deze oplossing sluit het beste aan bij de wensen van Oosterberg. Op het moment dat de organisatie zover is om ook gedrag en bestand en account-permissiewijzigingen te gaan monitoren, kan hier de uitbreiding Splunk UBA voor worden ingezet. Bedrijfscontinuïteit wordt behaald door het inzetten van de SIEM-oplossing en door het volgen van ISO 27001 A.12.4 Logging & Monitoring requirements. Hier wordt beschreven hoe logintegriteit gegarandeerd kan worden, waardoor forensisch onderzoek uitvoeren mogelijk wordt. Ook kan het monitoren optimaal en centraal worden ingericht als het opzetten van een SOC gerealiseerd wordt. In dit Security Operations Center werken securityspecialisten aan het analyseren en verwerken van beveiligingsmeldingen. In verband met de complexiteit van SIEM en de beperkte tijd en securityfuncties die Oosterberg (niet) heeft kan zowel het implementeren als het beheren van de oplossing het beste uitbesteed worden. Het uitbesteden wordt in dit geval behaald door een MSSP als partner te laten fungeren. Het is wel van groot belang dat er dan wel duidelijke SLA-afspraken worden gemaakt i.v.m. de verantwoordelijkheid op basis van meldingen, constateringen en te ondernemen acties. Op het moment dat deze stappen gevolgd worden dan wordt risicomanagement mogelijk gemaakt, businesscontinuïteit gegarandeerd en komt Oosterberg daarmee op een hoger beveiligingsvolwassenheidsniveau.

De conclusie:

Waardeoordeel

In eerste paar maanden van het traject werd er steeds verder van de eisen van Oosterberg afgegaan. Zowel ICT-Manager als de Infra-beheerder gaven dit aan en de onderzoeker had dit zelf ook door. Naarmate het project langer duurde is het onderzoek bijgedraaid in overleg met Oosterberg en kreeg de onderzoeker te horen dat het resultaat positief is. Volgens begeleiders van Oosterberg "Ziet het er goed uit" en de onderzoeker sluit zich hier bij aan. Het proces had echter beter kunnen verlopen. Op het moment dat er meer tijd was geweest dan waren er meerdere scenario's uitgewerkt, was er verder ingedoken op kosten en baten en was 'de beste SIEM-oplossing' veel eerder onderzocht.

Advies

De adviezen aan Oosterberg kunnen met de onderstaande bulletpoints geformuleerd worden:

- Er wordt aanbevolen om te beginnen met het formuleren van een log retentiebeleid
- Er wordt aanbevolen om Splunk Enterprise Security te gebruiken als SIEM-oplossing
- Er wordt aanbevolen om Splunk (ES) te laten implementeren door een partner en deze partner als MSSP te laten fungeren om Oosterberg accurate en tijdige meldingen te geven middels een SOC-platform
- Er wordt aanbevolen om goed na te denken over alle dimensies van een SLA als er met een partner gewerkt gaat worden
- Er wordt aanbevolen om een uitgebreid onderzoek naar een SOC uit te voeren
- Er wordt aanbevolen om een apart onderzoek uit te voeren naar UEBA
- Er wordt aanbevolen om de UBA-oplossing van Splunk te integreren nadat de oorspronkelijke oplossing een tijd staat en geconfigureerd is i.v.m. optimalisatie van Splunk Enterprise Security
- Wanneer er in de toekomst meer security en beheer in eigen huis zal komen, wordt er aanbevolen om hier trainingen voor te geven, te faciliteren en/ of gespecialiseerde security medewerkers aan te nemen. Hierbij draait het om de rollen en functies CISO, Security Analist en/ of SOC-medewerker(s).

10 Reflectie

Inleiding

De scriptie wordt afgerond met een reflectie over het gehele afstudeertraject. Hierbij wordt er begonnen met een algehele en overkoepelende reflectie, waarna er gereflecteerd wordt op wat belangrijke momenten tijdens het afstuderen. Tot slot wordt er kort gereflecteerd op de persoonlijke leerdoelen.

Zoals reeds bekend is het doel van Oosterberg: monitoring inzetten om op een hoger beveiligings- volwassenheidsniveau te komen. Hierbij zijn er een aantal concepten die centraal staan binnen dit project, namelijk: Monitoring, Security en Business. Deze onderdelen zijn op minimale wijze toegelicht in het leerpakket wat ik gedurende mijn ITSM-opleiding heb gehad. Dit brengt een hoop nieuwe uitdagingen met zich mee en deze uitdaging ben ik niet uit de weg gegaan. Ik heb enorm veel geleerd van deze periode, op zowel technisch als persoonlijk gebied. Daarnaast begaf ik mij ook in een vrij unieke begeleiding situatie en was het aan mij om hier mee om zien te gaan. Ik heb overwogen om deze ervaring buiten de reflectie te laten, maar door de impact die het op het project en mijzelf heeft gehad, reflecteer ik hier toch graag op.

Stageproces & Begeleiding

Het is normaal gesproken de bedoeling dat er een plan van aanpak met een planning wordt gemaakt en dat er gesprekken worden gevoerd met voortgangsrapportages. In deze voortgangsrapportages worden de volgende vragen gesteld en beantwoord:

- Wat is er in de afgelopen week uitgevoerd?
- Welke problemen kwam ik tegen?
- Hoe zijn deze problemen opgelost?
- Wat staat er voor volgende week op de planning?

Ooit is dit project herleidbaar op deze manier uitgevoerd, maar werd deze methode steeds minder aangehouden door een gebrek aan tijd. Dit komt omdat mijn oorspronkelijke begeleiding op z'n zachts gezegd een mismatch was. Hoewel de inhoudelijke informatie goed en informatief was, werd er voor mijn gevoel neerbuigend met mij gecommuniceerd. Al snel werd mijn vrije ingeving en regie minder en was ik het project alleen nog maar aan het uitvoeren voor en namens mijn begeleider. Dit zorgde voor een complete mismatch als het gaat om de wensen vanuit de begeleider van Saxion en de eisen die Oosterberg stelde. Dit heb ik geprobeerd op te pakken door continu te overleggen met beide partijen om toch een middenweg zien te vinden, maar intern voelde dit als een onmogelijke opgave. Veel van het werk dat ik opleverde was volgens mijn begeleider op meerdere onderdelen fout en ik ben wel 3 maanden bezig geweest om alleen maar revisies te verwerken. Voortgang was hierdoor nergens in zicht en mijn zelfvertrouwen begon wat af te nemen. Met nog maar vier weken voor de conceptuele oplevering had ik alleen nog maar een vooronderzoek, nog geen literatuurstudie en laat staan een ontwerp.

Richting het einde van het project werden de volgende dingen aan mij verteld:

- Vroegtijdig werd aangegeven dat ik het toch niet ging redden
- Het project was veel te groot en ingewikkeld om te halen voor de zomervakantie
- Dat ik de nodige kennis niet heb om dit project goed uit te kunnen voeren
- Dat ik aan een andere standaard werd gehouden dan medestudenten omdat mijn begeleider als een van de enige wist hoe er op het juiste competentieniveau gewerkt moest worden
- Tot slot werden er namen van andere docenten genoemd die er "helemaal niets van snappen en op verkeerd niveau werken"

De opsomming van punten was het laatste gesprek dat ik heb gevoerd met de begeleider voordat ik de situatie ging escaleren. Ik heb mijn knelpunten en perspectief geprobeerd te overleggen, maar dit gaf weinig resultaat. Toen heb ik tijdig besloten om dit te overleggen met mijn studieloopbaanbegeleider.

Dit 'escalatieproces' was absoluut de juiste zet en het is razendsnel opgepakt door alle betrokken personen en partijen. Hier ben ik enorm dankbaar voor. Samen met mijn nieuwe begeleider (Esther) heb ik meer vertrouwen gekregen in mijn werk.

Om te reflecteren op de afronding van deze afstudeerperiode ben ik trots op wat ik heb gemaakt en heb uitgevoerd. Toch had ik graag meer structuur gewild tijdens het afstuderen, door onder andere voortgangsrapportages te kunnen gebruiken. Ik denk dat dit een positieve invloed had kunnen hebben op de manier van onderzoeken en op de structuur van mijn documentatie. Kortom is deze periode zowel op academisch als persoonlijk gebied zeer leerzaam geweest.

Belangrijke situaties

Tijdens het gehele proces zijn er een aantal belangrijke momenten geweest die impact hebben gehad op het proces, scriptiestructuur of mijn manier van werken. Deze worden in dit onderdeel per moment beschreven.

<u>Toepasbare kennis</u>

Tijdens mijn studie heb ik meerdere methodieken op theoretische wijze leren toepassen op fictieve casussen. Ik vond het enorm leerzaam (en leuk) om dit in een groot bedrijf met een grote omgeving toe te passen. Het uitwerken van meerdere grote architecturale modellen, het verbinden van business en techniek en het gebruiken van UML in de praktijk was erg interessant.

Projectscope & competenties

Aan het begin van mijn scriptie ben ik begonnen met de competentieniveaus: analyseren, adviseren en realiseren. Door te onderzoeken kwam ik erachter dat een SIEM-oplossing implementeren (of realiseren) niet realistisch is binnen de beschikbare tijd. Uit mijn literatuurstudie komt het advies dat het uitbesteed moet worden i.v.m. complexiteit. Hierdoor veranderde de inrichting van de scriptie en ben ik aan het ontwerpen geslagen. Dit is een goede keuze geweest omdat ik hierdoor veel meer onderbouwde aanbevelingen kan geven.

Daarnaast is er door de manier waarop het project is verlopen geen duidelijke projectscope geweest die ik kon volgen. Mijn projectscope is het zoeken naar monitoringsconcepten en dit toepassen en verwerken in de bestaande omgeving van Oosterberg. Ik wilde veel verschillende scenario's modelleren en met elkaar vergelijken. Achteraf is het uitwerken van deze scenario's niet gelukt i.v.m. tijdsnood. Ik ben in overleg gegaan met mijn begeleider(s) van Oosterberg en heb besloten om alleen nog het advies met een alternatief uit te modelleren.

Monitoring → SIEM

Vanuit de beginfase van dit project is er gekeken naar de conceptuele mogelijkheden omtrent monitoring. Hierdoor zijn standaarden, strategieën en technische mogelijkheden bijvoorbeeld onderzocht. Dit zorgde er echter ook voor dat er geen pakketselectie is uitgevoerd naar de beste SIEM-oplossing. De uiteindelijke aanbeveling vanuit de literatuurstudie is het inzetten en gebruiken van een SIEM. In overleg met Oosterberg is er in de ontwerpfase vastgesteld dat er een grotere focus komt te liggen op SIEM en een minder grote focus op 'kortetermijnoplossingen' en overige concepten. Hierdoor is er als het ware een extra onderzoek uitgevoerd tijdens de ontwerpfase. Om de leesbaarheid te waarborgen is er in overleg met Esther besloten om dit naar voren te schuiven in het document en dit als apart document aan te leveren.

Security assessment

Tot slot wil ik het uitgevoerde security assessment samen met Mitchel Ponsioen nog even genoemd hebben. Dit assessment diende als vervanging van een prototype om zo het (technisch) ontwerp te concluderen. Nadat er was vastgesteld dat deze controlemethode gebruikt zou gaan worden, ben ik er snel achteraan gegaan. Mitchel kon op zeer korte termijn nog met mij aan tafel (via Teams) en het assessment verliep uitermate goed. Niet alleen was Mitchel inhoudelijk tevreden over wat ik al had uitgevoerd, ook de informatie over de onderdelen die nog extra aandacht nodig hadden was erg informatief. Ik begon aan dit assessment met de verwachting dat het een uurtje zou duren, terwijl er twee uur ingepland stond. We hebben er zonder onderbrekingen uiteindelijk bijna 4 uur van gemaakt en het is geen enkel moment oninteressant of waardeloos geweest. Mitchel toonde erg veel interesse in wat ik te zeggen had en zelf heb ik erg veel geleerd van wat Mitchel te zeggen had. Hoewel niet alle benoemde punten verwerkt kunnen worden i.v.m. de scope en tijd binnen dit project, zal ik ze absoluut meenemen voor toekomstige projecten.

Persoonlijke leerdoelen

Aan het begin van deze periode heb ik twee leerdoelen voor mijzelf geformuleerd. Dit zijn aandachtspunten waar ik extra hard mijn best op wil doen, met het uitgangspunt om er iets van te leren.

Duidelijkheid tijdens vergaderingen:

In het verleden heb ik niet altijd punten genoteerd voordat ik ging vergaderen. Dit leidde ertoe dat er bij anderen in de vergadering onduidelijkheid ontstond. Ik ben tijdens het afstuderen continu bezig geweest om mijn punten te noteren voor de vergadering en goed te luisteren naar input van anderen. Voor mijn gevoel is dit erg goed verlopen. Ik kon duidelijk mijn bevindingen uitten en op doordachte manier vragen stellen, terwijl de structuur en 'rode draad' van het overleg gevolgd kon blijven worden door alle betrokkenen.

Omgaan met onduidelijkheden:

Onduidelijkheden komen altijd voor en een belangrijk onderdeel is hoe er geacteerd wordt tijdens een onduidelijkheid. Onduidelijkheden kwamen in dit project het meeste op momenten voor waarbij ik contact nodig had met een stakeholder of begeleider. Contact leggen was het probleem niet, maar wachten op de afspraak wel. Om te voorkomen dat ik vastzat en niets kon doen heb ik deze onduidelijkheden opgepakt door ander werk op te pakken. Zo kon ik zelfstandig aan het werk blijven en laten zien dat deze momenten mij niet in de weg zitten. Overige onduidelijkheden pakte ik op door vragen te stellen aan collega's en begeleiders.

11 Bibliografie

27001 Academy. (2016, oktober 10). *How to integrate COSO, COBIT and ISO 27001 frameworks*. Opgehaald van 27001 Academy: https://advisera.com/27001academy/blog/2016/10/10/how-to-integrate-coso-cobit-and-iso-27001-frameworks/

27001 Academy. (2021). *What is ISO 27001?* Opgehaald van Advisera: https://advisera.com/27001academy/what-is-iso-27001/

AT&T. (2021). *AlienVault Products*. Opgehaald van Cybersecurity: https://cybersecurity.att.com/products/usm-anywhere/how-it-works

Axelos. (2019). *What is PRINCE2?* Opgehaald van Axelos Global Best Practise: https://www.axelos.com/best-practice-solutions/prince2/what-is-prince2

BMC Software. (2020, mei 13). *ITIL incident management*. Opgehaald van BMC Blogs: https://www.bmc.com/blogs/itil-v3-incident-management/

Boer, D. d. (2015). Wat is monitoring. Enschede.

Bouman, E. (2008). *SmarTEST.* Academic Service.

Bresser, A. (2020, oktober 30). Architectuur Review.

Chrissy Kidd. (2019, maart 7). *Tracing vs Logging vs Monitoring: What's the Difference?* Opgehaald van BMC: https://www.bmc.com/blogs/monitoring-logging-tracing/

CIO. (2017, juli 31). *What is IT governance? A formal way to align IT & business strategy*. Opgehaald van CIO: https://www.cio.com/article/2438931/governanceit-governance-definition-and-solutions.html

Dan Reichert. (2018, januari 5). *Logs and Metrics: What are they, and how do they help me?* Opgehaald van Sumo Logic: https://www.sumologic.com/blog/logs-metrics-overview/

Dnsstuff. (2020, mei 22). *What is Syslog*. Opgehaald van Dnsstuff: https://www.dnsstuff.com/what-is-syslog

DOEN. (2021). *Change kaleidoscope diagnosemodel*. Opgehaald van DOEN organisatieontwikkeling: https://doen-oo.nl/change-kaleidoscope/

Elastic. (2021). *SIEM at the speed of Elasticsearch*. Opgehaald van Elastic: https://www.elastic.co/siem

Eriksen-Coats. (2018, april 23). *what is mendelows matrix and how is it useful*. Opgehaald van oxford college of marketing: https://blog.oxfordcollegeofmarketing.com/2018/04/23/what-is-mendelows-matrix-and-how-is-it-useful/

Fowler, M. (2003). *UML Distilled third edition - A Brief Guide to the STandard Object Modeling Language.* Pearson Education.

Fruhlinger, J. (2018, mei 8). *What is a CSO? Understanding the critical chief security officer role*. Opgehaald van CSO Online: https://www.csoonline.com/article/2122505/what-is-a-cso-understanding-the-critical-chief-security-officer-role.html

Glen. (2020, december 1). *CISO Vs CSO: What Do They Mean?* Opgehaald van CISO Portal: https://www.ciso-portal.com/ciso-vs-cso-what-do-they-mean

Groot, M. d. (2021, mei 19). Vertegenwoordiger. (B. Franck, Interviewer)

Haveman, K., Hageraats, E., & Linden, S. v. (2016, september). Ontwerponderzoek. Enschede. Opgehaald van Blackboard.

IBM. (2021). *IBM QRadar SIEM*. Opgehaald van IBM: https://www.ibm.com/products/qradar-siem

ISO.org. (2021). *ISO/IEC 20000 ITSM*. Opgehaald van ISO OBP: https://www.iso.org/obp/ui/#iso:std:iso-iec:20000:-1:ed-3:v1:en

LiveAction. (2021). *Network Monitoring Protocols*. Opgehaald van Live Action blogs: https://www.liveaction.com/blog/types-of-network-monitoring-protocols/

LogPoint. (2021). *LogPoint as a cybersecurity solution*. Opgehaald van LogPoint: https://www.logpoint.com/en/solutions-industries/cybersecurity-solution/

LogRhythm. (2021). *LogRhythm NextGen SIEM Platform*. Opgehaald van LogRhythm: https://logrhythm.com/products/nextgen-siem-platform/

ManageEngine. (2016). *A guide to configure agents for log collection in EventLog Analyzer*. Opgehaald van ManageEngine.

ManageEngine. (2021). *Agentless Network Monitoring*. Opgehaald van ManageEngine: https://www.manageengine.com/network-monitoring/agentless-network-monitoring.html

ManageEngine. (2021). *EventLog Analyzer*. Opgehaald van ManageEngine: https://www.manageengine.com/products/eventlog/features.html

McAfee. (2021). *Enterprise Security Manager (ESM)*. Opgehaald van McAfee: https://www.mcafee.com/enterprise/en-us/products/enterprise-security-manager.html

McAfee. (2021). *What is a security operations center (SOC)?* Opgehaald van McAfee enterprise: https://www.mcafee.com/enterprise/en-us/security-awareness/operations/what-is-soc.html

Meenarani Rani. (2019). *IT Enterprise Monitoring Strategy*. Opgehaald van University of Missouri: http://www.umsl.edu/~sauterv/analysis/6840_f09_papers/Rani/Analysis.htm

Menten, B. (2021, mei 20). Sales vertegenwoordiger Fox-IT - MSSP, SOC en Splunk. (B. Franck, Interviewer)

Microsoft. (2021). *Azure Sentinel*. Opgehaald van Microsoft: https://azure.microsoft.com/en-us/services/azure-sentinel/#features

Midland Information Systems. (2021). *QRadar on Cloud SIEM*. Opgehaald van Midland information systems: https://www.midlandinfosys.com/qradar-cloud-siem-saas.html

Modi, H. (2019). *Enterprise IT Monitoring Strategy*. Opgehaald van Infosys - Experience transofromation : https://www.infosys.com/services/experience-transformation/documents/it-monitoring.pdf

Muravu, N. (2020, mei 31). *Strategic Change Management*. Opgehaald van Researchgate: https://www.researchgate.net/figure/The-Change-Kaleidoscope-Source-Balogun-Hope-Hailey-2004-The-change-kaleidoscope_fig2_341913436

NCSC. (2021). *SOC inrichten*. Opgehaald van Nationaal Cyber Security Centrum: https://www.ncsc.nl/aan-de-slag/richt-een-soc-in

NIST. (2021). *Information security continuous monitoring*. Opgehaald van csrc: https://csrc.nist.gov/glossary/term/information_security_continuous_monitoring

Oosterberg. (2021). *Missie en Visie*. Opgehaald van Oosterberg: https://www.oosterberg.nl/wie-zijn-wij/missie-visie-en-kernwaarden/

Opengroup. (2021). *The TOGAF Standard*. Opgehaald van Opengroup: https://www.opengroup.org/togaf

O'Reilly. (2021). *The Three Pillars of Observability*. Opgehaald van oreilly: https://www.oreilly.com/library/view/distributed-systems-observability/9781492033431/ch04.html

Phil Winder. (2020). *Logging vs Tracing vs Monitoring*. Opgehaald van Winderresearch: https://winderresearch.com/logging-vs-tracing-vs-monitoring/

Ponsioen, M. (2021, mei 27). Managing Director Wazda. (B. Franck, Interviewer)

Raza, M. (2020, mei 27). *Introduction to IT Monitoring*. Opgehaald van BMC Blogs: https://www.bmc.com/blogs/it-monitoring/

Raza, M. (2020, juli 7). *The Chief Information Security Officer (CISO) Role Explained*. Opgehaald van BMC: https://www.bmc.com/blogs/ciso-chief-information-security-officer/

Segovia, A. J. (2015, november 23). *Logging and monitoring according to ISO 27001 A.12.4*. Opgehaald van 27001 Academy: https://advisera.com/27001academy/blog/2015/11/23/logging-and-monitoring-according-to-iso-27001-a-12-4/

Sigma Groep. (2021). *Root Cause Analysis*. Opgehaald van Lean Agile en Six Sigma: https://leansixsigmagroep.nl/lean-agile-en-six-sigma/root-cause-analysis/

SolarWinds. (2021). *Automate SIEM Log Aggregation, Analysis and Reporting*. Opgehaald van SolarWinds: https://www.solarwinds.com/security-event-manager/use-cases/siem-monitoring-tool

SolarWinds MSP. (2020, maart 10). *SIEM vs. Log Management*. Opgehaald van Solarwinds: https://www.solarwindsmsp.com/blog/siem-vs-log-management#

Splunk. (2020, januari 13). *Metric and Log Monitoring: Do You Really Need Both?* Opgehaald van Splunk: https://www.splunk.com/en_us/blog/devops/metric-log-monitoring-really-need.html

Splunk. (2021). *Compare SPlunk Security Analytics vs. Tradition SIEM* . Opgehaald van Splunk: https://www.splunk.com/en_us/resources/videos/splunk-for-security-vs-siem.html

Splunk. (2021). *Components of a Splunk Enterprise deployment*. Opgehaald van Splunk: https://docs.splunk.com/Documentation/Splunk/8.2.0/Capacity/ComponentsofaSplunkEnterprisedeployment

Splunk. (2021). *Email notification action*. Opgehaald van Splunk Alerting Manual: https://docs.splunk.com/Documentation/Splunk/8.2.0/Alert/Emailnotification

Splunk. (2021). *Reference Hardware*. Opgehaald van Splunk: https://docs.splunk.com/Documentation/Splunk/8.2.0/Capacity/Referencehardware

Splunk. (2021). *Splunk Data-ToEverything Pricing*. Opgehaald van Splunk: https://www.splunk.com/pdfs/getting-started/splunk-data-to-everything-pricing.pdf

Splunk. (2021). *SPlunk Enterprise architecture and processes*. Opgehaald van Splunk: https://docs.splunk.com/Documentation/Splunk/8.2.0/Installation/Splunksarchitectureandwhatgetsinstalled

Splunk. (2021). *What is IT Monitoring*. Opgehaald van Splunk: https://www.splunk.com/en_us/data-insider/what-is-it-monitoring.html

Stone, J. (2021). *What are HIPAA compliant system logs*. Opgehaald van Security metrics: https://www.securitymetrics.com/blog/what-are-hipaa-compliant-system-logs

Sumo logic. (2021). *Log analyse*. Opgehaald van Sumologic: https://www.sumologic.com/glossary/log-analysis/

Sumo Logic. (2021). *SIEM vs Log Management*. Opgehaald van Sumologic: https://www.sumologic.com/glossary/siem-log/

Tek-Tools. (2020, mei 4). *Network Monitoring: Protocols, Best Practices, and Tools*. Opgehaald van Tektools Networks: https://www.tek-tools.com/network/network-monitoring-guide-and-tools

TU Delft. (2020, november 5). *Causalerelatiediagram*. Opgehaald van TUDelft: https://sysmod.tbm.tudelft.nl/wiki/index.php/Causalerelatiediagram

Vliet, H. v. (2007). *Software Engineering: Principles and Practice.* Opgehaald van http://15.222.11.163/wp-content/uploads/2020/01/Software-Engineering-Principles-and-Practice.pdf

12 Bijlages

12.1 Bijlage 1: Behoefteanalyse

Stakeholderanalyse

Een stakeholderanalyse (ofwel belanghebbendenanalyse) zorgt ervoor dat er tijdens een project juist en concreet wordt aangegeven welke betrokken/ belanghebbenden partijen 'key players' zijn in het project. Deze key players hebben bijvoorbeeld veel zeggenschap en krijgen zo de meeste prioriteit tijdens het project. Om dit juist weer te geven wordt de analyse uitgevoerd op basis van de matrix van Mendelow (Eriksen-Coats, 2018). Er worden bij de matrix vier categorieën gehanteerd, zodat er gepast gehandeld kan worden.

Om tot een goede verdeling en indeling te komen van de belanghebbenden, worden de stakeholders (belanghebbenden) vanuit een brainstormsessie uitgewerkt in een longlist. Deze longlist wordt door de analyse verkleind tot een shortlist. Diezelfde shortlist wordt vervolgens ook gebruikt bij de probleemanalyse.

Longlist

Er wordt eerst bedacht wie er eventueel allemaal belang bij dit project kan hebben. Uit deze brainstormsessie is de volgende longlist gekomen:

- Koninklijke Oosterberg B.V.
  - ICT-Manager
  - ICT-Beheerders
    - Systeembeheerder(s)
    - Infrastructuurbeheerder(s)
    - Applicatiebeheerder(s)
    - Project en procesbeheerder(s)
  - Financiën
  - Directie
  - Personeelszaken
  - Systeemgebruikers
- ICT-support partijen
  - Wazda
  - Bradon
  - Het-IT
- Overig
  - Overheid (AVG)
  - Klanten

Stakeholder macht en interesse analyse

		Interesse	
		Laag	Hoog
Macht	Laag	• Systeemgebruikers • Overheid • Klanten • Personeelszaken • Financiën	• Wazda • Bradon
	Hoog	• N.v.t.	• Directie • ICT-Manager • Systeembeheerder • Infrastructuurbeheerder

Tabel 20 Macht en Interesse vergelijkingsanalyse

Lage macht & lage interesse:

- Systeemgebruikers
  - Het project is gericht op de interne processen en systeemobjecten van de ICT-omgeving. Het heeft geen invloed op de werkwijze van Systeemgebruikers. De gebruikers hebben hierdoor geen interesse in het project en de gebruikers hebben ook geen macht om het project te wijzigen of stop te zetten.
- Overheid
  - Dit project heeft geen staatsgeheimen en behandelt/ bewerkt ook geen persoonsgegevens, dus is de AVG niet van toepassing. Er is weinig interesse in een losstaand project bij Oosterberg en er is ook geen macht om dit project stil te zetten.

- Klanten
    - Dit project heeft geen invloed op de webshop en persoonsgegevens. Het project is gericht op de interne processen en systeemcomponenten/ objecten. Er is geen interesse in een achtergrondproject bij de ICT van Oosterberg en het project kan ook niet door klanten gewijzigd worden.
- Personeelszaken
    - Personeelszaken hebben weinig interesse en macht omdat er niet omgegaan wordt met personeelsgegevens. Naast dit onderdeel worden ze ingedeeld op dezelfde wijze als de Systeemgebruikers.
- Financiën
    - Financiën hebben bij dit project weinig macht omdat deze investeringen en verantwoording direct vanuit de directie komt. Interesse is er om deze zelfde redenen niet.

Hoge interesse & lage macht:

- Wazda
    - Wazda is een IT-supportpartij die Oosterberg met ingewikkelde ICT-projecten helpt. Daarnaast is Wazda betrokken bij het meedraaien in het infrastructuurteam. Ook het helpen en leiden in mogelijke reputatieschade als er dingen niet goed geregeld zijn, zijn onderdelen die Wazda oppakt. Uit persoonlijke gesprekken blijkt dat de ingehuurde krachten van Wazda interesse hebben bij de uitkomst van dit project. Dit komt met name door de persoonlijke interesse, naast het feit dat er eventueel gewerkt zal worden met de aanbevelingen/ uitkomsten van dit project. De macht is daarentegen laag omdat er geen rol is waarbij er invloed kan worden uitgevoerd op dit project. Hierdoor wordt Wazda ingedeeld op een hoge interesse, maar lage macht.
- Bradon
    - Bradon is ook een IT-supportpartij die Oosterberg helpt met ingewikkelde ICT-projecten. Bradon wordt niet ingehuurd om dagelijks mee te draaien in het infrastructuurteam. Interesse is hoog omdat er gewerkt zal worden met de aanbevelingen/ uitkomsten van dit project. Macht is daarentegen laag omdat er als support-partij geen macht uitgeoefend kan worden op dit project.

Lage interesse & hoge macht:

- N.v.t.

Hoge interesse & hoge macht:

- Directie
    - Omdat het project zich afspeelt omtrent ICT-processen en omgeving, heeft de directie veel interesse en macht. Er kan sturing worden gegeven indien wenselijk en de uitkomsten van dit project komen direct bij de directeur en manager terecht. Het project komt voort vanuit de ICT-afdeling, maar als directie aangeeft dat er bijvoorbeeld geen belang meer is bij het project, kan er een stop op het project worden gezet.
- ICT-Manager
    - De manager staat het dichts bij dit project en de uitkomst van het project. Het project kan stopgezet worden, er kan gestuurd worden en er kunnen eisen en wensen gewijzigd/ toegevoegd worden. Daarnaast zijn er soms dagelijks en minimaal wekelijkse voortgangsvergaderingen om aan te tonen wat de status is van het project.
- Systeembeheerder
    - De systeembeheerder ervaart direct wat de uitkomsten van dit project zijn. Alle nazorg en opvolging komt ook bij deze belanghebbende terecht. Vanuit dit perspectief is er daarom veel interesse en ook macht. Hoewel de macht tussen directeur en systeembeheerder onderling uiteraard op verschillende niveaus ligt, kan er zeker sturing worden gegeven.

- Infrastructuurbeheerder
    - De infra-beheerder staat net als de manager het dichts bij dit project en de uitkomst van het project. Het project kan stopgezet worden, er kan gestuurd worden en er kunnen eisen en wensen gewijzigd/ toegevoegd worden. Daarnaast zijn er soms dagelijks en minimaal wekelijkse voortgangsvergaderingen om aan te tonen wat de status is van het project.

Behoeften van belanghebbenden

De behoeften van belanghebbenden zijn verkregen d.m.v. het toepassen van semigestructureerde interviews. De interviews worden op deze wijze afgenomen om zo gerichte vragen te kunnen stellen, waarna er verder gevraagd kan worden en zo meer informatie vergaard kan worden.

Directie

De directie is verantwoordelijk voor de goed- of afkeuring van het project. Als lid van de directie en stem van de ICT-afdeling kan de ICT-Directeur aangeven waar de ICT-afdeling prioriteiten heeft liggen, wat er speelt op de afdeling en waar Oosterberg in de toekomst naartoe gaat of zou moeten gaan. Een belangrijke rol van de ICT-directeur is het meenemen van de rest van de directie in het belang van dit project en zo de directie medeverantwoordelijk maken. Zo kan er ook duidelijk worden gemaakt dat dit project meer prioriteit heeft dan andere projecten. Tot slot kan ook het geluid vanuit de directie terug worden vertaald/ gebracht naar de ICT-afdeling en/ of ICT-manager. Hoewel de organisatie gezien wordt als platte organisatie met informele sfeer, kan de directie sturing geven aan het project door vanaf een hoge functie een uniek perspectief te bieden. Overkoepelende eisen en wensen komen hieruit voort. Procesgericht werken is een uitgangspunt, waarbij ICT inmiddels koste wat kost “gewoon moet werken”. Uit het interview kunnen de volgende eisen en wensen worden vastgesteld:

- De omgeving dient een uptime te blijven houden van 99%
- Er moet op basis van een juist kosten en baten overzicht gestreefd worden naar een zo hoog mogelijke beschikbaarheid van de omgeving
- De oplossing dient bij te dragen aan procesgericht-werken
- De oplossing dient indien mogelijk bij te dragen aan meetbaar projectgericht-werken
- Er moeten trendanalyses uitgevoerd kunnen worden, waar rapportages uitgehaald moeten kunnen worden
- Bij de zoektocht naar een oplossing dient er duidelijk gemaakt te worden waarom er wel of niet voor Cloud gekozen moet worden
- Vervolgstappen a.d.h.v. dit project dienen inzichtelijk gemaakt te worden
- De oplossing dient Oosterberg naar een hoger beveiligingsvolwassenheidsniveau te brengen

Infrastructuurbeheerder

De Infrastructuurbeheerder heeft een enorm belangrijke rol binnen dit project. Met de primaire belangen bij de veiligheid en beschikbaarheid van de omgeving van Oosterberg, kan deze belanghebbende met juiste onderbouwing de juiste eisen en wensen aanleveren. De Infrastructuurbeheerder is vooral bezig met het uitvoeren van projecten, waarbij er in de recente jaren meer focus ligt op het beveiligingen van de omgeving. Eisen en wensen zijn uit diverse interviews gehaald en staan hieronder vernoemd:

- Rapportages op basis van analyses dienen geleverd te kunnen worden
- Als er gekeken wordt naar een technische oplossing, dient er rekening te worden gehouden met de bandbreedte en performance van de bestaande omgeving
- Historische data dient beschikbaar te worden gemaakt
- Er dient meer te worden gelogd dan alleen het essentiële, maar er is nog onduidelijk wat dit exact zou moeten worden
- Er dienen analyses op basis van trends uitgevoerd te kunnen worden
- Er dient meer inzicht en historie te komen op de events en logging van systemen, waarbij de primaire focus ligt op security(-events)
- Er dient iets te worden ingericht waardoor we van onze logging ‘verzamelbak’ afkomen
- Een technische oplossing dient alomvattend te zijn, alle apparatuur dient in een oplossing te komen
- Er dient een beheervriendelijke oplossing te komen
- De ICT-afdeling dient niet overspoeld te worden met gegevens
- Configuratie dient plaats te kunnen vinden a.d.h.v. templates
- Opvolging van events dient op simpele wijze gedaan te kunnen worden
- Het kunnen afvinken van events zou erg mooi zijn

ICT-Manager

De link tussen ICT-Directeur, ICT-medewerkers en de sturing van dit project ligt bij de ICT-Manager. Vanuit wellicht de belangrijkste en meest impactvolle rol in dit project, ziet de ICT-manager uiteraard graag dat dit project slaagt. Dit project zal vanuit het perspectief van de manager slagen wanneer de onderstaande eisen en wensen behaald worden. Deze eisen zijn verkregen via meerdere uitgevoerde interviews:

- (Log)data dient compacter, meer gecentraliseerd en verfijnd te worden opgeslagen

- De oplossing dient goed ingebed te kunnen worden in het nieuwe beheerplan
- De oplossing moet trendanalyses uit kunnen voeren om verbanden inzichtelijk te maken
- Er dient zichtbaar te worden dat er een hacker binnen is en waar deze is geweest
- Er dient op welke manier dan ook zichtbaar te worden wat een hacker heeft verkregen, zowel op data als rechtenniveau
- Er dient meer proactief gewerkt te kunnen worden door bijvoorbeeld bedreigingen tijdig te kunnen signaleren
- De oplossing dient niet te complex te zijn
- Een oplossing dient indien/ voor zover mogelijk gescheiden te worden van bestaande infrastructuur i.v.m. beveiliging en beschikbaarheid
- Er dient duidelijk te worden gemaakt hoelang logs bewaard dienen te worden
- Een mogelijke oplossing dient een goede voorziening te hebben om te kunnen filteren en zoeken
- De oplossing dient eventherkenning te hebben om te zien welke events wanneer voor komen
- Er dienen 'severity scores' gehangen te kunnen worden aan events die belangrijker zijn en meer prioriteit verdienen
- Er dient systeemherkenning te zijn op basis van merk of type, waarbij een mogelijke tool weet dat iets bijvoorbeeld een 'HP core switch' is
- Het signaleren en analyseren van events en mogelijke kwetsbaarheden dient ook te kunnen gebeuren a.d.h.v. templates
- Indien mogelijk moet er inzichtelijk worden gemaakt wat best practices omtrent monitoring zijn
- Een oplossing dient zowel on premise als in de Cloud logs op te kunnen halen
- Een oplossing dient een ingebouwd managementsysteem te hebben om events en alerts te kunnen managen
- Het zou mooi zijn als er iets komt dat geïntegreerd kan worden met TopDesk, als integratiemogelijkheden niet bestaan dient de oplossing dit zelf op te pakken
- Er dient onderzocht te worden wat er allemaal gelogd zou kunnen worden
- Trends moeten geanalyseerd en herkent kunnen worden
- De oplossing dient Oosterberg naar een hoger beveiligingsvolwassenheidsniveau te brengen

<u>Systeembeheerder</u>

De systeembeheerder zal a.d.h.v. dit project wellicht de meeste gevolgen ervaren. Mogelijke en toekomstige proceswijzigingen en de aanpassing of toevoeging van technische voorzieningen komen allemaal direct op de afdeling terecht. Vanuit het uitgevoerde interviews komende onderstaande eisen en wensen terug:

- (Log)data dient relevant te worden, het is nu te irrelevant en in te grote bulk
- Firewalls, routers en overige netwerkcomponenten dienen beter inzichtelijk te zijn
- Onduidelijkheden omtrent logging dienen voor zover mogelijk verholpen te worden
- Bedrijfscontinuïteit moet verhoogd worden door de verhoging van het beveiligingsniveau
- Potentiële oplossingen dienen geautomatiseerd ingezet te kunnen worden
- Potentiële oplossingen dienen gebruiksvriendelijk (of beheervriendelijk) te zijn
- Er dient rekening te worden gehouden met de complexiteit van een of meerdere oplossingen

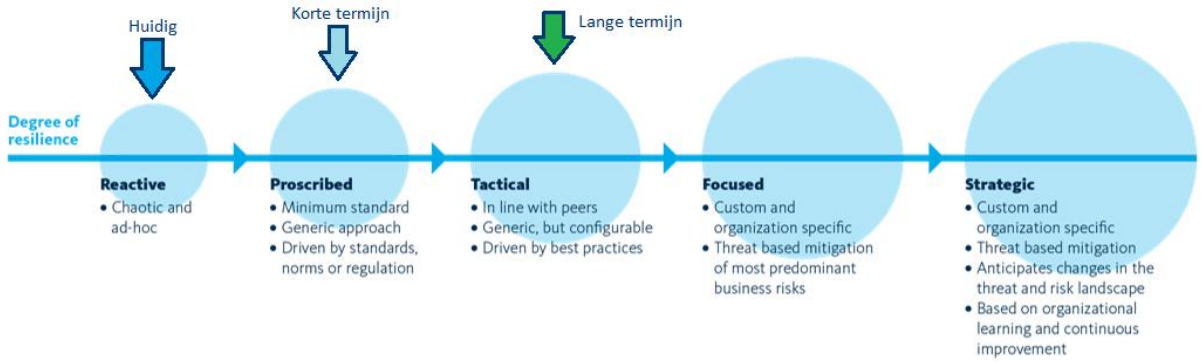
Er dient rekening te worden gehouden met de impact op de omgeving i.v.m. de gelimiteerde bandbreedte

12.2 Bijlage 2: Contextanalyse

Huidige volwassenheidsniveau

Onderstaande afbeelding geeft de verschillende niveaus aan waarop een organisatie zich kan bevinden, wanneer er gekeken wordt naar de weerstand van een ICT-afdeling/ organisatie. Deze afbeelding geeft ook direct weer in welk stadium Oosterberg zich momenteel bevindt.

Oosterberg begeeft zich nu in een reactieve omgeving, waarbij er ad hoc gereageerd en beheerd wordt.



Figuur 33 Volwassenheidsniveaus ICT (Bresser, 2020)

De nabije toekomst (2020/ 2021) geeft de korte termijn weer. Oosterberg is druk bezig om dit niveau te bereiken door een hoop veranderingen door te voeren. Dit betreft het implementeren van diverse nieuwe oplossingen omtrent security, logging en het opzetten van een operationeel beheerplan.

Op de lange termijn (2021 en later) is het de bedoeling dat Oosterberg het 'Tactical' niveau gaat behalen. Dit kan alleen gedaan worden op het moment dat alle onderdelen die gevonden zijn in het security assessment, aangepakt worden. Tactical is daarom ook de gewenste situatie. Een van de onderdelen die op de planning staat voor deze lange termijn, is het opzetten van een monitoring (en logging) oplossing, een Syslog of een SIEM-oplossing zijn hier voorbeelden van. Het vaststellen van de daadwerkelijke (monitoring)problemen en behoeften zal bijdragen aan het maken van de juiste beslissing. Het zal een doel zijn om aan te kunnen tonen welke behoeften er op korte en lange termijn behaald kunnen worden en op welke wijzen dit behaald kan worden. Aanbevelingen en alternatieven zullen beschreven moeten worden en onderbouwd moeten worden d.m.v. de juiste onderzoek conclusies en ontwerpen.

Toelichting kaleidoscope:
Tijd geeft aan op welke termijnen er eventueel interventies plaats kunnen vinden om bepaalde veranderingen door te voeren. Het gaat bij korte termijn over de acceptatie en bij de lange termijn over veranderingen in de cultuur. Omdat dit project nog niet afgerond en er nog niet duidelijk is welke veranderingen er eventueel plaats moeten nemen, kan er alleen maar geschat worden dat de acceptatieveranderingen maandelijks plaats kunnen vinden. Mogelijke culturele veranderingen kan bijvoorbeeld wel zes maanden voor worden genoteerd, maar is wellicht niet van toepassing op dit project.
Scope:
Dit project zal invloed hebben op de technische voorzieningen en mogelijk ook de werkwijzen van medewerkers. Door deze redenen wordt dit project opgesteld als een 'middelmatige organisatieverandering'. Uit interviews blijkt ook dat er wellicht een verandering in mindset nodig zal zijn. Niet alle collega's zitten op dezelfde lijn als het gaat om mogelijke veranderingen en zien niet allemaal dezelfde redenen om te moeten vernieuwen.
Preservation:
Dit onderdeel betreft het behouden van positieve aspecten in de huidige situatie. Bij Oosterberg zal positiviteit behouden moeten worden, waarbij negativiteit in dit geval uiteraard behandeld dient te worden. Daarbij zal er dicht bij de waarden en visie van Oosterberg gebleven dienen te worden.
Diversity:
Diversiteit geeft inzicht in de culturele verschillen in de organisatie, met de multidisciplinariteit die daarbij komt kijken. Dit project speelt zich af op de hoofdlocatie van Oosterberg en de culturele verschillen zijn echt aanwezig maar wordt op gemiddeld ingeschat. Dit komt door de verschillende teams en belanghebbenden bij de organisatie, er zijn veel verschillende subculturen per afdeling maar medewerkers hebben veelal dezelfde percepties en visie over projecten, werkzaamheden etc. Multidisciplinariteit is daarbij ook gemiddeld, er is veel verschillende kennis aanwezig in het bedrijf, maar de organisatie heeft een erg grote infrastructuur waarbij er externe partijen en specialisten worden ingezet om specifieke onderdelen in te richten.
Capability:
Dit onderdeel geeft aan of de medewerkers en de organisatie zelf klaar staat voor mogelijke veranderingen a.d.h.v. dit project. Uit interviews blijkt dat de meeste medewerkers klaar staan voor deze veranderingen, maar dat nog niet iedereen op dezelfde

lijn zit. De organisatie staat klaar voor de veranderingen, omdat Oosterberg op een hoger beveiligingsvolwassenheidsniveau wil komen en hier de juiste faciliteiten voor inzet en ingezet heeft.
Capacity:
De capaciteit geeft weer wat de status is van de onderdelen 'Geld, Mensen en Tijd'. De status van deze onderdelen wordt beschreven zoals ze zijn ten tijde van het ontwerpen van de kaleidoscope en verwacht wordt dat deze status gedurende de rest van het project gelijk zal blijven.
Bij Oosterberg kunnen de volgende onderdelen gesteld worden:

- Geld: hoog, omdat er geen budget is bij dit project en er wordt aangegeven dat mogelijke kosten geen showstopper zullen en mogen zijn (mits de kosten en baten overeenkomen).
- Mensen: neutraal, omdat er niet te veel of te weinig medewerkers zijn.
- Tijd: laag, omdat er ondanks een heldere planning met korte en lange termijn doelen een gebrek is aan de tijdsvoorziening om alles juist te kunnen oppakken. Uit interviews en persoonlijke gesprekken blijkt dat de medewerkers van de ICT-afdeling het erg druk hebben.

Readiness:
Het is van belang dat alle betrokken partijen klaar zijn om te veranderen. Dit project speelt zich af op de ICT-afdeling, maar er zijn ook belanghebbenden die zich niet direct op de ICT-afdeling bevinden.
ICT heeft de status 'high' gekregen omdat het project vanuit hier ontstaan is. Overig personeel staat op neutraal omdat er eerst verduidelijking zal moeten komen wat de mogelijke impact op hun werkzaamheden is.
Power:
Dit onderdeel benoemd alle belanghebbenden bij dit project. Daarnaast wordt aangegeven of er een wijziging in autonomie is. Belanghebbenden bij dit project zijn: Directeur groot aandeelhouder, ICT-directeur, ICT-manager, Infrastructuurbeheerder en Systeembeheerder.

- Autonomie**:**
    - Verwacht wordt dat er weinig wijzingen zijn omtrent de autonomie van de medewerkers. Dit project geeft niet meer zeggenschap of vrijheid en is gericht op processen, werkwijzen en de infrastructuur van de organisatie.

Binnenste cirkel – oorsprong van het project en veranderingen:
Dit onderdeel beschrijft de binnenste cirkel. Hierin staan de afrondende conclusies en aanbevelingen beschreven die in gewenste situatie gevolgd worden om mogelijke organisatieveranderingen tot een mooi en succesvol einde te brengen. Het sturen naar een succesvol einde kan in sommige situaties het beste worden opgepakt door het uitvoeren van zogenoemde 'interventies'. Deze interventies vormen samen uiteindelijk een interventieplan, maar zal voor dit project buiten de scope vallen en kan worden gezien als mogelijke nazorg.
Interventie toelichting:
Interventies worden een zevental categorieën ingedeeld en zullen per 'change' in worden gedeeld. Om het compact te houden worden niet alle mogelijke interventies per nummer toegelicht.

1 De groep op koers brengen
2 Leren van elkaar stimuleren
3 Gesprekinterventies
4 Gespreksvormen
5 Bijeenkomsten als interventie
6 Structuurveranderingen als interventietechniek
7 Vergaarbak, overige interventies

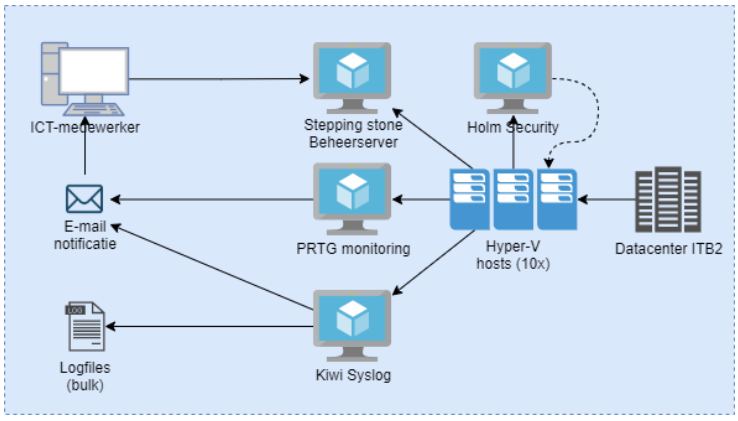
Change path: Adaptation change
Adaptation is gekozen omdat er op een specifiek onderdeel van de organisatie en infrastructuur een project wordt uitgevoerd dat aangepast dient te worden. [3]
Change start point: Bottom up change
Bottom up is gekozen omdat de verandering/ het project vanuit de ICT-afdeling is ingezet en niet vanuit een Top-down aanpak is ingezet. [1] [5]
Change style: Collaboration style
Collaboration is gekozen omdat de veranderingen niet vanaf boven door worden gevoerd en er samengewerkt zal moeten worden om tot een juist projecteinde te komen. [2] [3]
Change target: Output
Output is gekozen omdat het is de bedoeling is dat monitoring wordt ingezet om het beveiligingsvolwassenheidsniveau te verhogen. [7]

Logging bij Oosterberg

Onderstaande informatie is verkregen door schriftelijke communicatie met de infrastructuurbeheerder, systeembeheerder en persoonlijke interviews.

Een korte tijd geleden is er een minimale logging-oplossing ingezet, dit d.m.v. de tool 'Kiwi Syslog' van Solarwinds. De tool wordt ingezet om alle logs- en events van beide core switches en firewalls op te halen. Daarnaast wordt het momenteel ook ingezet om de 'Failure' status op te halen van de security audits op de Management-server 2 (SVR-MGT-02).

Het ophalen van deze logs is pure en ruwe data, er worden momenteel alleen mails naar het e-mailadres gestuurd van de afdeling automatisering op het moment dat er foutieve inlogpogingen zijn op de systemen. Er is momenteel een overkoepelend operationeel beheerplan in ontwikkeling, maar op dit moment wordt er nog niets met de opgehaalde data gedaan. Dit beheerplan beschrijft wat er per situatie verwacht wordt van de diverse betrokken partijen, op het moment dat er bepaalde acties ondernomen dienen te worden. Het staat nog niet op de planning om hier tot in detail monitoringsprocessen in te beschrijven. Dit is echter wel benodigd want meten is weten.
PRTG is ook sinds kort nog uitgebreider ingezet. Alle 98 servers staan in deze monitoringoplossing, hoewel het nog strakker geoptimaliseerd en ingericht kan worden. Sommige sensoren staan nog op de standaard ingestelde waarden vanuit de autodiscover functionaliteit en een aantal overige losse sensoren zullen i.v.m. de groei nog strakker ingesteld moeten worden.
De hypervisors hebben een security logboek in PRTG staan d.m.v. wmi-sensoren, deze geven een alert op het moment dat er foutief wordt ingelogd. Sinds kort staat het eventsecurity-logboek van VM's ook in PRTG.
Tot slot is er recent ook een project gaande omtrent het scannen naar kwetsbaarheden. Het scannen naar kwetsbaarheden op apparatuur en software wordt nu gedaan door de oplossing van Holm Security. Deze tool scant continu naar kwetsbaarheden (CVE's) op de infrastructuur.
Onderstaande figuur visualiseert de beschreven informatiestroom in de huidige situatie (daadwerkelijke componenten, koppelingen en technische aspecten worden niet in dit document behandeld en staan in het technisch ontwerp).



Figuur 34 Globale huidige situatie

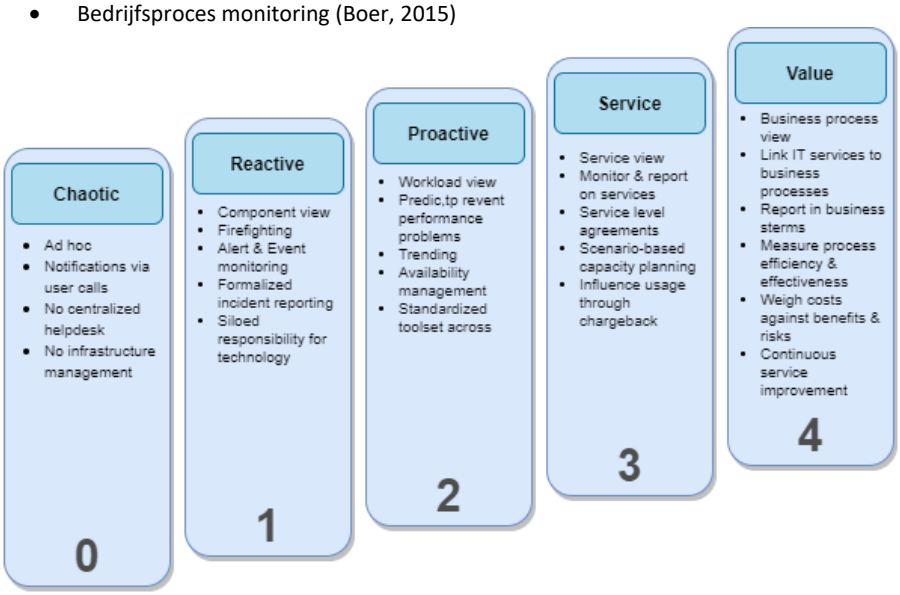
Volwassenheidsniveau van monitoring

Het algemene volwassenheidsniveau van Oosterberg is uiteraard al in kaart gebracht, maar nu is het nog wel van belang dat er gekeken wordt naar het specifieke volwassenheidsniveau van monitoring bij Oosterberg. Normaliter wordt dit geformuleerd als uitgangspunt bij het opstellen van een ICT-beleidsplan. Het ICT-beleid staat echter niet tekstueel beschreven, dus zal het lastig worden om vanuit die invalshoek concreet te formuleren op welk niveau monitoring zich bevindt bij Oosterberg. Hierdoor kan niet methodisch worden vastgesteld wat het daadwerkelijke monitoringsvolwassenheidsniveau is.

Middels de persoonlijke gesprekken die zijn gehouden en de uitgevoerde deskresearch, kan de onderstaande wel worden vastgesteld:

Volwassenheidsstadia worden vaak onderkent op (minimaal) de volgende onderdelen:

- Component monitoring
- ICT-service monitoring
- Bedrijfsproces monitoring (Boer, 2015)



Figuur 35 Monitoring volwassenheidsmodel (Boer, 2015)

Het bovenstaande model geeft weer op welke niveaus monitoring bij een organisatie zich kan begeven. In verband met de wens om meer trendanalyses te kunnen doen en hierover rapportages te krijgen, kan er gesteld worden dat Oosterberg ernaar streeft om minstens het tweede (proactieve niveau) te behalen. Dit sluit goed aan bij de algemene doelstelling: om op een hoger (tactisch) beveiligingsvolwassenheidsniveau te komen.

Er wordt ad hoc actie ondernomen op bevindingen, maar bevindingen komen niet alleen vanuit gebruikers binnen want monitoren op actuele status wordt namelijk al wel uitgevoerd. In de monitoringoplossing (PRTG) van Oosterberg wordt continu gekeken naar de status van apparatuur binnen de infrastructuur. Daarnaast bestaat er al wel een centrale helpdesk, is er al infrastructuur management en kunnen individuele componenten inzichtelijk worden gemaakt. Oosterberg bevindt zich tussen een chaotische en reactieve monitoringomgeving, maar omdat er geen daadwerkelijk niveau kan worden vastgesteld, kan het beste vanaf niveau 0 naar boven worden gewerkt. Dit betreft het component monitoring, oftewel de monitoring van de technologie (Boer, 2015).

Tot slot kan hieruit geconcludeerd worden dat het van belang is voor de organisatie, dat er op technisch gebied, met name op de onderdelen logging en reporting wordt ingezoomd. Het monitoren van actuele status van netwerkapparatuur wordt met een snel tempo verbeterd, het optimaliseren van PRTG is een apart project wat Oosterberg parallel aan dit project al heeft opgepakt. Aan de organisatorische kant zal uit het (voor)onderzoek moeten blijken hoe de mogelijkheden tegenover de eisen en wensen van Oosterberg staan.

12.3 Bijlage 3: Literatuurstudie

Three pillars of observability

In de hedendaagse ICT-wereld evolueert alles continu, het moment dat (ICT)organisaties stilstaan dan gaat men in feite achteruit door de enorme sprongen die de techniek maakt. De meest gebruikte en nieuwe concepten in de wereld van monitoring zijn 'Metrics' en 'Tracing'.

Logs, metrics en tracing staan bekend als de "Three pillars of observability" oftewel, de drie pillaren van waarneembaarheid. Hoewel het duidelijk is dat alleen de toegang tot deze drie concepten niet voldoende is om iets 'waarneembaar' te maken, zijn er krachtige tools die (wanneer goed begrepen) ervoor kunnen zorgen dat er mogelijkheden zijn om systemen te verbeteren (O'Reilly, 2021).

Metrics

Metrische gegevens zijn een numerieke weergave van gegevens gemeten over tijdsintervallen. Metrics kunnen de kracht van wiskundige modellering en voorspelling benutten om kennis af te leiden van het gedrag van een systeem over momenten van zowel het verleden als de toekomst (O'Reilly, 2021). Metrics worden vaak gebruikt in situaties waarbij een organisatie een cloud omgeving heeft waar applicaties, virtuele servers en services worden gebruikt. Oosterberg maakt gebruik van een Microsoft Azure omgeving, waarbij momenteel o365, AzureAD en Dynamics 365 worden gebruikt. Monitoringsoplossingen hebben vaak een basis gebaseerd op logs of metrics. Hierbij worden metrics meestal gebruikt om gebruikte resources en performance in de gaten te houden. Als gekeken wordt naar de voornaamste verschillen van bronnen, dan kan hierin de onderstaande korte opsomming worden gemaakt (Splunk, 2020):

Populaire metric bronnen:

- System metrics (CPU, memory, disk)
- Infrastructure metrics (AWS CloudWatch)
- Web tracking scripts (Google Analytics)
- Application agents (APM, error tracking)

Populaire log bronnen:

- System logs (syslog, journald)
- Application logs (log4j, log4net)
- Server logs (Apache, MySQL)
- Platform logs (AWS CloudTrail)

"A log is an event that happened and a metric is a measurement of the health of a system" (Dan Reichert, 2018).

Moderne monitoringsoplossingen kunnen ervoor zorgen dat de lijn tussen 'metric' en 'log' wordt ingekort. Meestal is het belangrijk dat er wordt begonnen met logging, waarna er altijd nog uitgebreid kan worden d.m.v. metrics. Wat wel van belang is dat er begrepen moet worden dat logging, tracing en metrics en/ of monitoring een representatie is van welke acties er door een softwareoplossing worden uitgevoerd. Het draait er dus niet om wat de software doet, maar dat er begrepen wordt hoe de software zich gedraagt (Chrissy Kidd, 2019). Er is vaak niet een goed antwoord als het gaat om 'wat in te zetten, logs of metrics?'. In veel gevallen zullen organisaties op korte of lange termijn beiden nodig hebben. Voor Oosterberg zal het echter het meest interessant zijn om een start te maken met logs en nog even te wachten met het invoeren van metrics, zonder metrics volledig aan de kant te zetten. Dit komt omdat het project in eerste instantie gericht is op beveiliging en niet op performance.

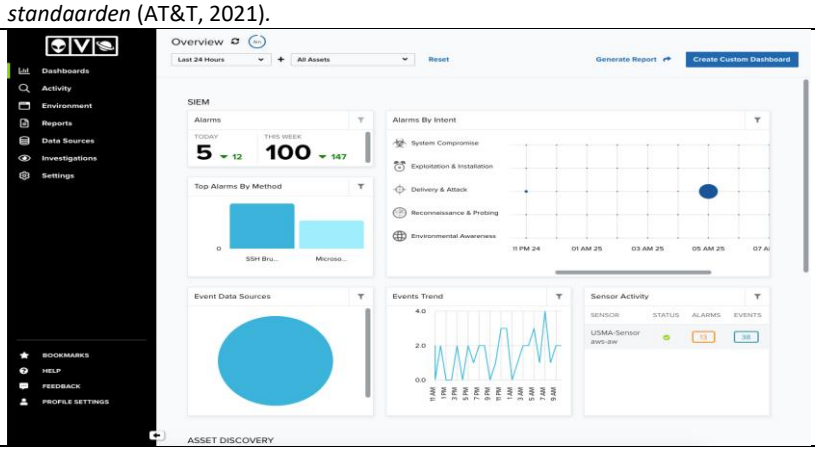
Figuur 36 De doeleinden van Logs & Metrics (Dan Reichert, 2018)

Tracing

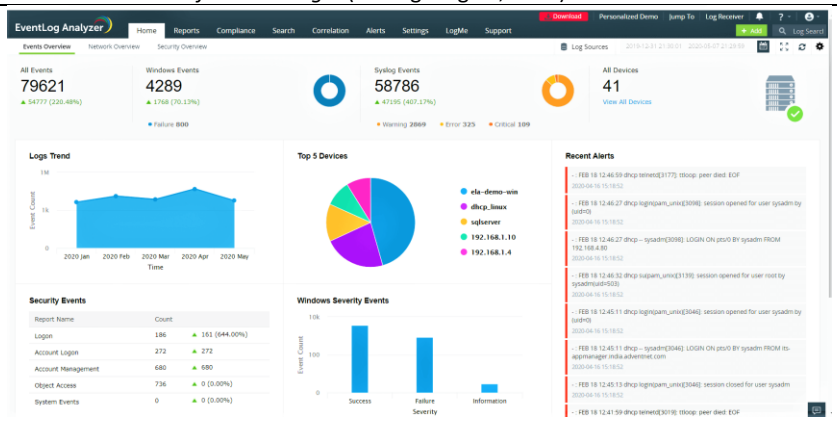
Tracing (ofwel traceren) is een weergave van een reeks causaal gerelateerde gebeurtennissen die van begin- tot eindpunt een 'verzoek/ verzoekstroom' vanuit een systeem coderen. Tracing is onderdeel van de 'pillaren van waarneembaarheid' en is zo dicht gerelateerd aan metrics. Echter valt het behandelen van tracing buiten de scope van dit project omdat het gericht is op het volgen (traceren) van een enkele gebruiker en de weg die deze gebruiker aflegt. Het concept van deze 'weg' is in dit geval een applicatielandschap en het doel van tracing is over het algemeen performance (Phil Winder, 2020).

12.4 Bijlage 4: Pakketselectie

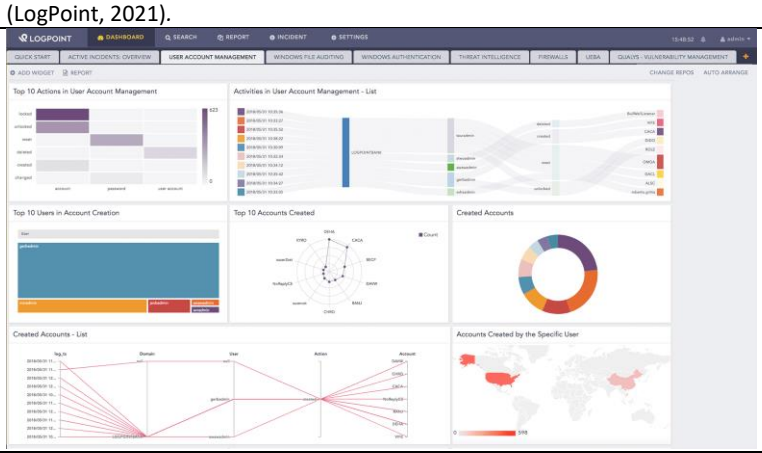
Oplossingen

Naam	***AlienVault USM Anywhere***
Bedrijf	*AT&T Cybersecurity*
Type	*Closed Source*
Beschrijving	*Het bedrijf AT&T Cybersecurity is een van de grootste Managed Security Services Providers (MSSP). Het bedrijf levert producten om cybersecurity aan te pakken en om daarmee impact op businesscontinuïteit onder controle te houden. Het bedrijf levert twee AlienVault producten, USM en OSSIM. Hierbij is USM Anywhere een uitgebreidere versie en niet open source, maar closed source. AlienVault OSSIM kan niet worden ingezet voor Oosterberg omdat het geen Log Management features heeft. USM Anywhere verzamelt en analyseert automatisch data en stelt dit centraal beschikbaar zonder hier complexiteit aan te hangen. De oplossing wordt automatisch geüpdatet en zo is een ICT-afdeling altijd bij met de nieuwste mogelijke bedreigingen. Daarnaast is het mogelijk om acties te automatiseren, ook in samenwerking met andere securityoplossingen. Hierdoor kunnen mogelijke incidenten snel opgepakt worden.* *AT&T Cybersecurity gebruikt een dedicated single-tenant datastore architecture die speciaal wordt ingezet om monitoringdata veilig te stellen. Het maakt gebruik van het TLS protocol om veilige verbindingen tot stand te zetten, op deze data wordt encryptie uitgevoerd met een AES 256-bit key. De oplossing werkt met zowel on premise als Cloud omgevingen, heeft geen hardware nodig om Cloud te kunnen monitoren en gebruikt een sensor om on premise, virtuele omgevingen en Cloud omgevingen te kunnen monitoren. Dit zijn 'agents' die geïnstalleerd dienen te worden op betreffende componenten. Op apparatuur zoals routers en switches is het mogelijk om 'agentless' te monitoren, door via beveiligde TCP SSH poort 22 data te controleren.* *Het bedrijf garandeert veiligheid van data door te voldoen aan PCI DDS Level 1, HIPAA en SOC 2 Type 2 standaarden* (AT&T, 2021).
Home interface voorbeeld	

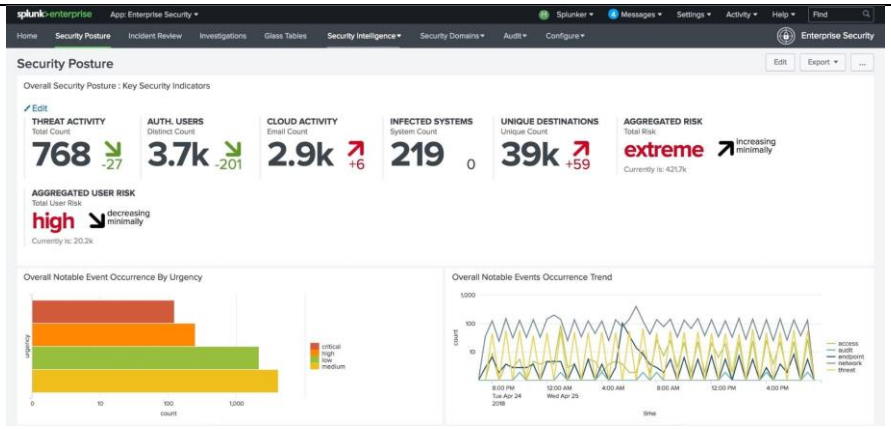
Tabel 21 AlienVault USM Anywhere (AT&T, 2021)

Naam	***EventLog Analyzer***
Bedrijf	*ManageEngine*
Type	*Closed Source*
Beschrijving	*ManageEngine is de IT-divisie van de 'Zoho Corporatie'. Het doel van ManageEngine is om diverse pakketten met verschillende features aan te bieden, zodat alle klanten met zowel groot als klein budget een oplossing kunnen vinden. Het bedrijf heeft inmiddels meer dan 90 producten, waarvan de EventLog Analyzer het product is en onder andere als SIEM fungeert. Het product kan echter veel meer dan 'alleen' SIEM. Het levert Log Management, Applicatie auditing, Netwerk auditing, IT Compliance, SIEM en Cross-Platform auditing. Alle typen logs en log management kunnen worden opgepakt door de EventLog Analyzer, waar SIEM vervolgens de forensische gegevens van kan analyseren. De oplossing is web-based en haalt informatie van alle belangrijke componenten op (routers, switches, UNIX, Syslog, Windows) door gebruik te maken van een agent-less of agent-based architecture. Dit kan geïnstalleerd worden op een Linux of Windows machine. De web client kan benaderd worden door te browsen naar de hostnaam van de machine waar het op draait met de gebruikte poort. Er kan gebruikt worden gemaakt van lokale autorisatie, een Radius-server of Domein-login* (ManageEngine, 2021).
Home interface voorbeeld	

Tabel 22 EventLog Analyzer (ManageEngine, 2021)

Naam	***LogPoint***
Bedrijf	*LogPoint*
Type	*Closed Source*
Beschrijving	*LogPoint is een Deens bedrijf dat 'gedreven is om de beste SIEM-oplossing in de wereld te maken'. Het bedrijf voegt SIEM samen met UEBA (User and Entitiy Behavior Analytics) en probeert zich zo te onderscheiden op gebied van cybersecurity, compliance, IT-operations en business analytics. De oplossing LogPoint staat 24/7 klaar om ondersteund te worden door support voor partners en klanten. De oplossing kan worden opgedeeld in een drietal modules: Collectors, Backend en de Search head. De Collectors zorgen voor het verzamelen, normaliseren en verrijken van de data. De Backend is een NOSQL-storage oplossing die ervoor zorgt dat alle data op basis van een 'flat file' wordt opgeslagen en daardoor gemakkelijk opgezocht kan worden. Dit garandeert ook access control door de integratiemogelijkheden die deze setup biedt en zorgt voor lage- tot geen performance impact. Wanneer gekozen wordt voor de Cloud variant kan bijvoorbeeld ook Office365 in log management gezet en geanalyseerd worden. LogPoint geeft aan dat een holistische weergave van de gehele omgeving van een organisatie van groot belang is en dat de SIEM-oplossing LogPoint hieraan bijdraagt. Het bedrijf voldoet aan ISO-standaarden, UK GPG13 en de GDPR* (LogPoint, 2021).
Home interface voorbeeld	

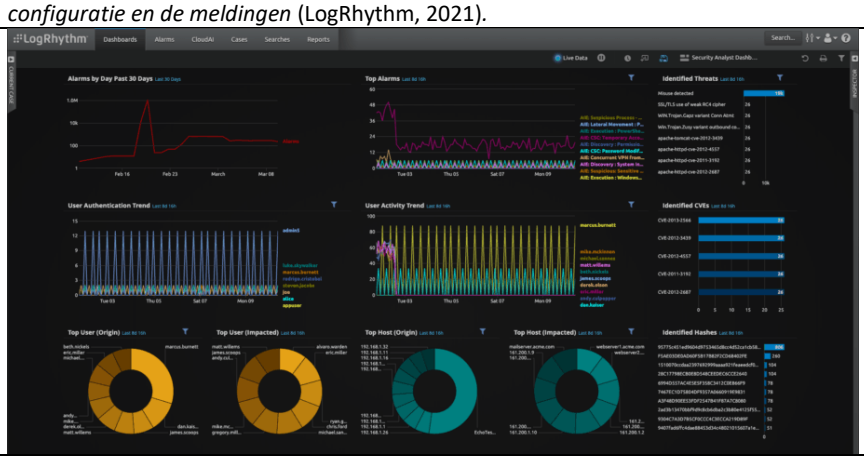
Tabel 23 LogPoint (LogPoint, 2021)

Naam	***Splunk Enterprise Security***
Bedrijf	*Splunk*
Type	*Closed Source*
Beschrijving	*De grootste/ een van de grootste SIEM leveranciers in de ICT-wereld is Splunk. De oplossing die het bedrijf levert, geeft echter meer dan alleen een 'traditionele SIEM'. Het bedrijf wil zich onderscheiden op de markt door aan te geven dat een traditionele SIEM niet meer altijd voldoende is. Splunk vergelijkt een traditionele SIEM met een boot vol met belangrijke data. Op deze boot doe je alles om je data te beveiligen: Lijnen met haken uitgooien om alle bedreigingen op te vissen voordat ze bij de data komen. "Dat is een SIEM"* (Splunk, 2021)*. Het probleem hier is echter dat er een moment komt dat een bedreiging niet bij de uitgegooide lijnen en parameters past. Daarnaast kan het ook nog eens voorkomen dat er een kwaadwillige collega toegang heeft tot alle data. De oplossing van Splunk kan gezien worden als complete sonar van 'de gehele oceaan' in plaats van alleen 'de boot met lijnen'. Splunk Enterprise Security heeft een applicatie nodig om data te verzamelen, deze kan op een server geïnstalleerd worden en benaderd worden via een beveiligde https-link of middels een onbeveiligde HTTP link* (Splunk, 2021).
Home interface voorbeeld	

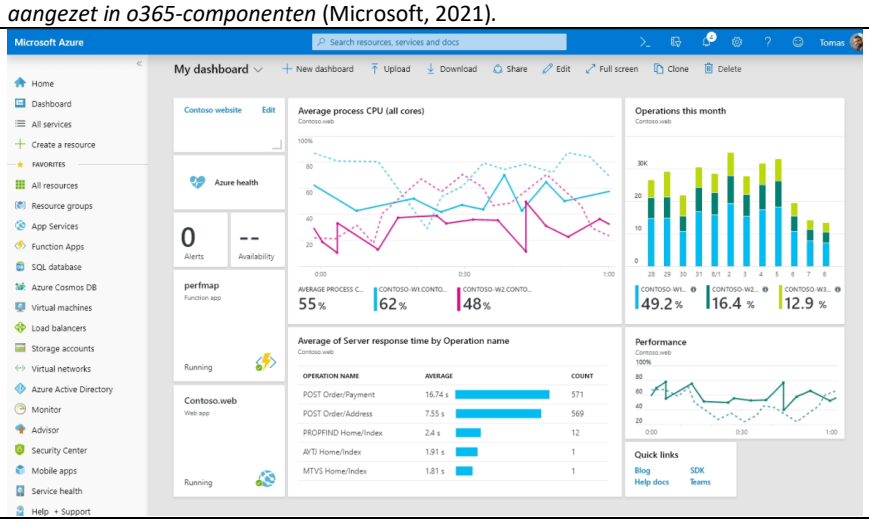
Tabel 24 Splunk Enterprise Security (Splunk, 2021)

Naam	***IBM QRadar SIEM***
Bedrijf	*IBM*
Type	*Closed Source*
Beschrijving	*QRadar SIEM van IBM is een oplossing die ervoor probeert te zorgen dat er een organisatie breed overzicht gecreëerd wordt. De oplossing kan zowel in de cloud als on premise worden opgezet. Dit wordt gedaan middels een hardware virtual appliance of een SaaS-oplossing die gehost wordt door IBM. Het voordeel van QRadar is de naadloze integratiemogelijkheden met andere IBM-producten. Op het moment dat het on premise gedraaid zal worden, dient het een aparte server te krijgen. In de cloud wordt het een geheel andere dienst/ oplossing. Hierbij geeft IBM aan dat het een SIEM as a Service is (MSAAM/ SIEMaaS). Net als bij de meeste Cloud oplossingen is hiervan het voordeel dat alles automatisch geüpdatet wordt en dat schaalbaarheid gegarandeerd is. IBM levert bij de Cloud oplossing 24/7 infrastructuur onderhoud en support* (Midland Information Systems, 2021).
Home interface voorbeeld	

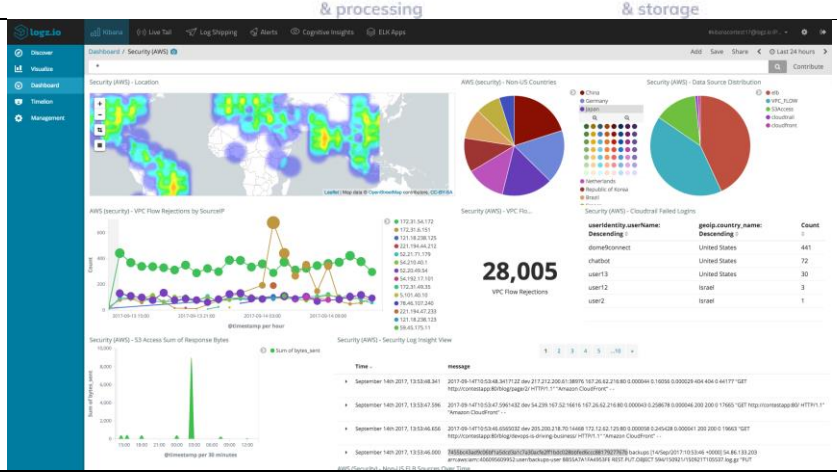
Tabel 25 QRadar SIEM (IBM, 2021)

Naam	***LogRhythm NextGen SIEM Platform***
Bedrijf	*LoghRythm*
Type	*Closed Source*
Beschrijving	*NextGen SIEM van LoghRythm levert een SIEM-oplossing die onderdelen zoals UEBA, NTA en SOAR samenvoegt. De oplossing kan worden verkregen in de vorm van een on premise, IaaS of MSSP-oplossing. LogRhythm wil ervoor zorgen dat de SIEM-oplossing klaar staat om een mogelijk SOC te ondersteunen. LogRhythm geeft aan dat de Cloud oplossingen vanzelfsprekend HA (high availability) hebben, maar ook dit kan geconfigureerd worden op de on premise omgeving. LogRhythm is sinds 2019 'pro cloud' en levert nu de service 'LogRhythm Cloud", wat de SIEM-deployment, onderhoud en infrastructuur regelt. Hierbij wordt alles van het NextGen SIEM Platform in de cloud geregeld en hoeft de klant alleen nog te letten op configuratie en de meldingen* (LogRhythm, 2021).
Home interface voorbeeld	

Tabel 26 LogRhythm NextGEN SIEM Platform (LogRhythm, 2021)

Naam	***Azure Sentinel***
Bedrijf	*Microsoft*
Type	*Closed Source*
Beschrijving	*De 'Cloud-native SIEM solution' van Microsoft. Microsoft Azure heeft als een van de eerste grote Cloud providers een Cloud-native SIEM gemaakt die naadloos geïntegreerd kan worden met Azure. De oplossing kan zowel met de Cloud-omgeving als met on premise omgevingen worden ingezet. De oplossing heeft integratiemogelijkheden met andere 'best-of-breed' producten door een REST-API te gebruiken. Sentinel is ook naadloos te integreren met o365, hiervoor moeten er wel een aantal log-functionaliteiten worden aangezet in o365-componenten* (Microsoft, 2021).
Home interface voorbeeld	

Tabel 27 Azure Sentinel (Microsoft, 2021)

Naam	***Elastic (ELK) Stack***
Bedrijf	*Elastic*
Type	*Open Source*
Beschrijving	*Elastic is een Europees bedrijf met een hoofdlocatie gevestigd in Nederland (Amsterdam). De ELK Stack utility bestaat uit de samengevoegde tools: Logstash, Elasticsearch, Kibana en Beats. Het is een van de grootste open source oplossingen met enorm veel integratiemogelijkheden. Cisco, Azure, AWS, Fortinet en Microsoft 365 en Teams zijn een aantal voorbeelden. Kosten worden in dit geval gemaakt door support/ security-pakketten. De service die hiervoor afgenomen kan worden is Elastic Cloud. Op het moment dat alles 'self-managed' (ofwel in eigen beheer wordt genomen) dan is het gratis. Elastic heeft net als andere leveranciers partners die kunnen helpen bij implementatie of demo's. Officieel is het geen SIEM-oplossing, maar er zijn integratiemogelijkheden die het op een SIEM-oplossing kunnen laten lijken. Op het moment dat de oplossing op 'simpele wijze' in wordt gezet, dan ziet het er als volgt uit* (Elastic, 2021)*:* 
Home interface voorbeeld	

Tabel 28 Elastic ELK Stack (Elastic, 2021)

Naam	***McAfee Enterprise Security Manager***
Bedrijf	*McAfee*
Type	*Closed Source*
Beschrijving	*De SIEM-oplossing van McAfee die zowel in de cloud als on premise kan draaien. "McAfee® SIEM solutions bring event, threat, and risk data together with an optimized user experience, leveraging the latest technology, open source, and McAfee and partner innovations to provide the strong security insights, rapid incident response, seamless log management, and compliance reporting required for optimized security operations."* (McAfee, 2021)
Home interface voorbeeld	

Tabel 29 McAfee Enterprise Security Manager (McAfee, 2021)

Naam	*SolarWinds Security Event Manager*
Bedrijf	*SolarWinds*
Type	*Closed Source*
Beschrijving	*Oosterberg heeft al producten van SolarWinds in de ICT-omgeving staan, maar SolarWinds heeft ook een SIEM-oplossing om aan te bieden. De Security Event Manager (SEM) (niet te verwarren met het security discipline SEM) is ontworpen om effectief logmanagement van Security Information and Event Management (SIEM) te vergemakkelijken. SEM is gebouwd met een SIEM-logboek verzameltool waarmee automatisch logboeken van meerdere apparaten en toepassingen in het netwerk van de organisatie verzamelt en samengevoegd kunnen worden. Dit wordt gedaan door een agent-less architectuur.* *SolarWinds probeert met hun Security Event Manager onderscheid te maken van de andere SIEM-oplossingen door een betaalbare en gebruiksvriendelijke oplossing beschikbaar te stellen* (SolarWinds, 2021).
Home interface voorbeeld	

Tabel 30 SolarWinds Security Event Manager (SolarWinds, 2021)

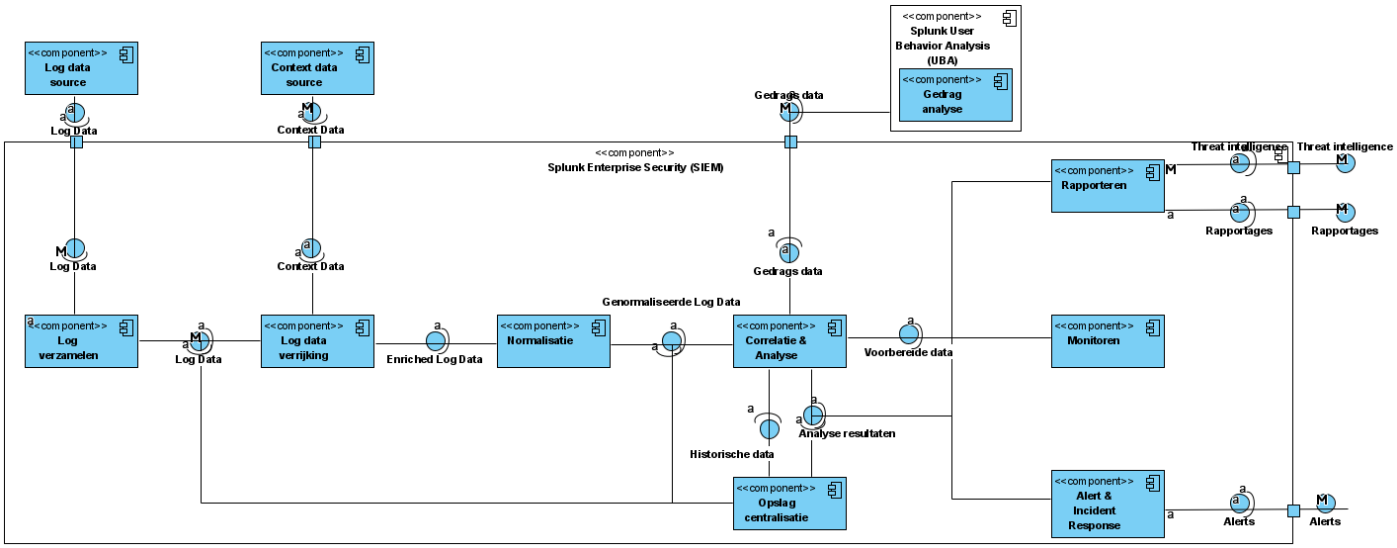
12.5 Bijlage 5: Functioneel ontwerp

Onderstaande tabel geeft weer welke log data er per kritieke asset van belang is.

Kritieke asset	Log data
Locus	Opslagcapaciteit van VM van Locus, back-up controle, status van TrendMicro Suite
Triathlon	Opslagcapaciteit van vm van ERP, back-up controle, status van TrendMicro Suite
Router	Uptime, aanvallen, inlogpogingen, configuratieveranderingen, systemhealth
Switch	Configuratie, configuratieveranderingen, systemhealth
WLAN	Uptime, ongeautoriseerde logins
Nimble	Systemhealth, vollopende LUN's (capaciteit), dient via host gemonitord te worden
Desktop Oost.	Foutieve sites en inlog, status virusscanner, aanwezigheid ransomware, bestandswijzigingen
Azure	Alerts over verdacht gebruik (bijvoorbeeld mails naar privé of te veel naar OneDrive). TrendMicro Cloud app security status.
Telefonie	-
E-Commerce	Locatie logins, inzicht in waar de liveomgeving draait
EDI Centric	Uptime, ongewone verbindingen en connecties, portal uptime (dit wordt nu middels PRTG gedaan)
MessageService	Inzicht in waar de verbindingen vandaan worden gemaakt (locatieherkenning)

Tabel 31 Log data kritieke assets

Onderstaande architectuurdiagram geeft aan wat de componenten van Splunk ES zijn en hoe deze aan elkaar zijn gerelateerd. Door dit ontwerp wordt er duidelijk welke componenten er allemaal in de oplossing zitten.
Component diagram:



Figuur 37 SIEM UML Component Diagram

12.6 Bijlage 6: Interviewvragen

Organisatievragen:

1. In welke sector bevindt Oosterberg zich?
2. Wat is de marktpositie van Oosterberg?
3. Wat is de strategie van Oosterberg?
4. Wat is de missie van Oosterberg?
5. Welke diensten en producten worden door Oosterberg geleverd en hoe wordt dit gedaan?
6. Wat is het aantal klanten dat Oosterberg heeft?
7. Bestaat er grote concurrentie in de sector van Oosterberg?
8. Hoe zou je de organisatie beoordelen met betrekking tot het naleven van eigen kernwaarden en zijn er punten die verbeterd worden?
9. Wat zijn de belangrijkste processen van de organisatie?
10. Wordt er veel samengewerkt met andere bedrijven? En hoe zit dit op gebied van ICT?
11. Hoeveel medewerkers heeft Oosterberg op haar hoofdlocatie, en hoeveel in totaal?
12. Hoe is de dynamiek en werkverdeling binnen de ICT-afdeling?
13. Bestaat er een beheerplan en hoe wordt deze nageleefd?
14. Wat is de processtroom van ICT-ontwikkelingen richting de goedkeuring van het management?
15. Zijn er organisatorische tekeningen beschikbaar?
16. Welke doelen stel jij voorop binnen de ICT-afdeling en omgeving?
17. Welke rapportages ontvang jij/ of zou je graag willen ontvangen omtrent ICT?
18. Welke primaire belangen heb jij zelf bij ICT-projecten?
19. Op welke gebieden zie jij zelf graag de ICT-afdeling en het ICT-landschap op positieve wijze wijzigen?
20. Bestaan er processen omtrent monitoren en het constateren van beveiligingslekken?

Leiderschap en cultuurvragen:

1. Hoe zou jij de manier van leiddinggeven beschrijven bij Oosterberg en verschilt dit per afdeling?
2. Wat is jouw manier van leiddinggeven?
3. Welke vaardigheden heb je volgens jou nodig om leiding te kunnen geven?
4. Hoe wil je dat er naar jou wordt gekeken als leidinggevende?
5. Geef je ook aan hoe er gecontroleerd wordt en op welke wijze er besluiten worden genomen?
6. Worden er gesprekken gevoerd met jouw personeel en zo ja, wat voor gesprekken zijn dit?
7. Heb je inspiratiebronnen als leider?
8. Wat zijn de leuke aspecten van leiderschap?
9. Wat zijn de lastige aspecten van leiderschap?
10. Heb je afrondend nog tips over leiddinggeven?

Technische vragen:

1. Wat is volgens jou de huidige status van logs- en events van infrastructuurcomponenten bij Oosterberg?
2. Welke problemen komt Oosterberg tegen in relatie tot de status van de aanwezigheid van logs- en events?
3. Wat is de huidige manier van werken en beheer, als het gaat om het detecteren van een potentiële hacker of data lek?
4. Is er een DLP-beleid en in hoeverre wordt deze nageleefd?
5. Tot hoever kan Oosterberg (historische) data terugzien van infrastructuurcomponenten?
6. Wat zijn de primaire belangen bij het implementeren van een monitoringoplossing voor Oosterberg?
7. Zijn er bepaalde veiligheids- of back-up regels waar Oosterberg zich aan houdt die van belang kunnen zijn bij het project?
8. Staan er grote wijzigingen op de planning omtrent de netwerkcomponenten die Oosterberg momenteel heeft?
9. Wat zijn vanuit jou eisen waaraan een monitoringoplossing zich moet voldoen?
10. Welke onderdelen van de infrastructuur worden momenteel geautomatiseerd bij Oosterberg?
11. Zijn er nog dingen die jij graag ziet gebeuren in de loop of tijdens de afronding van dit project?

12.7 Bijlage 7: Interview - Infrastructuurbeheerder

Interviewvragen worden opgedeeld in organisatievragen en technische vragen. Door vanuit dezelfde interviewer, dezelfde vragen aan verschillende belanghebbenden te stellen, worden er verschillende antwoorden gegeven. De antwoorden blijven zo, voor zover mogelijk, betrouwbaar en valide.

Organisatievragen

1. In welke sector bevindt Oosterberg zich?

Elektrotechnische groothandel, de detailhandel.

2. Welke diensten en producten worden door Oosterberg geleverd en hoe wordt dit gedaan?

Logistieke diensten, alle producten die gerelateerd zijn aan een elektronische groothandel.

3. Hoe zou je de organisatie beoordelen met betrekking tot het naleven van eigen kernwaarden en zijn er punten die verbeterd worden?

Goed, we denken in oplossingen. We zijn erg flexibel en we gaan erg met de markt mee. Ooit begonnen als pianobouwer en nu in de elektrotechnische groothandel. Onze kracht ligt daar absoluut, het mee willen met de markt en de klanten. De klanten hebben in het verleden wel eens leningen bij ons aangevraagd bijvoorbeeld. We steken onze nek uit voor klanten.

4. Wat zijn de belangrijkste processen van de organisatie?

We zijn geen ICT-bedrijf, maar het gaat steeds meer richting ICT, alle oplossingen moeten nu gemanaged worden. Een steeds groter deel wordt web georiënteerde dienstverlening. Daarom moet er steeds meer ICT-kennis bij komen kijken.

5. Wat zijn mogelijke ICT-technische bedreigingen voor het bedrijf?

Phishing mail, de hackpogingen en de ransomware. Bedrijfsdata die buit gemaakt kan worden en vooral juist gegijzeld kan worden.

6. Hoe is de dynamiek en werkverdeling binnen de ICT-afdeling?

Wij hebben een software development kant en infrastructuur kant, we zouden meer helpdesk (1^e, 2^e en 3^e lijn) moeten hebben.

7. Op welke gebieden zie jij zelf graag de ICT-afdeling en het ICT-landschap op positieve wijze wijzigen in de (nabije) toekomst?

Dat we dus meer naar een onderscheid tussen helpdesk en infra en software moeten. Het segmenteren van het netwerk moeten we naar toe en daarmee kunnen we beter de bandbreedte managen.

8. Bestaat er een beheerplan en hoe wordt deze nageleefd?

Hij bestaat niet maar hij bestaat wel in concept, dus hij wordt gemaakt nu. Hij wordt nu geschreven op de wijze zoals we het nu eigenlijk al doen, dus leven we het ook al na. Er komt nu alleen wel meer structuur in.

Technische vragen

1. Wat is volgens jou de huidige status van logs- en events van infrastructuurcomponenten bij Oosterberg?

Alleen de hoogst essentiële logging wordt gedaan, dit zijn de foute loginpogingen op de core-switches en firewalls. Dus we loggen wel, maar alleen het meest essentiële en dat is te weinig. Je kunt dus ook geen analyses doen op basis van trends en het inzien van historische data.

2. Welke problemen komt Oosterberg tegen in relatie tot de status van de aanwezigheid van logs- en events?

We hebben een forensisch onderzoek gehad, maar deze kon niet juist worden uitgevoerd. Dit kwam omdat er voldoende historische data aanwezig was.

3. Wat is de huidige manier van werken en beheer, als het gaat om het detecteren van een potentiële hacker of data lek?

Reactief op ontvangen alerts. Deze alerts komen van de nieuwe en niet volledig geoptimaliseerde syslog server en de security logs van de Hyper-V servers, met daarbij de management/ stepping-stone server.

4. Is er een DLP-beleid en in hoeverre wordt deze nageleefd?

Er is geen beleid, maar er is wel stukje DLP vanuit TrendMicro. Dit wordt toegepast op servers, computers, laptops en mail.

5. Tot hoever kan Oosterberg (historische) data terugzien van infrastructuurcomponenten?

Van de switches, routers en firewalls wordt geen logging opgeslagen. De switches hebben wel een configuratie die wordt opgeslagen. De events en logging van de firewalls en switches gaat nu wel naar de syslog server. Daar is nog geen auto-archive rule van.

6. Wat zijn de primaire belangen bij het implementeren van een monitoringoplossing voor Oosterberg?

Het verkrijgen van inzicht en historie op de events en logging van systemen. Het meest gericht op security-events vanuit Oosterberg. We willen meer kunnen dan alleen de verzamelbak van onze huidige situatie met de kiwi-syslog server, waarbij er geen trends en analyses met goede filtering opgezet kunnen worden.

7. Zijn er bepaalde veiligheids- of back-up regels waar Oosterberg zich aan houdt die van belang kunnen zijn bij het project?

Vanuit de back-up nee, het maakt niet uit waar de VM staat. Als uit een best practice blijkt dat SIEM apart data op moet slaan, dan maakt het wel uit waar bijvoorbeeld deze VM staat. Wat betreft capaciteit hebben we genoeg en we zijn momenteel bezig met de hardening van onze back-up.

8. Staan er grote wijzigingen op de planning omtrent de netwerkcomponenten die Oosterberg momenteel heeft?

Ja, dit jaar zouden de core-switches vervangen moeten worden. Hier komen we momenteel nog niet aan toe.

9. Wat zijn vanuit jou eisen waaraan een monitoringoplossing zich moet voldoen?

Het moet alomvattend zijn. Alle apparatuur moet er in kunnen, niet alleen Linux, of een router, of alleen een switch. Ik wil trends kunnen zien, historie kunnen zien voor forensisch onderzoek. Het moet beheers vriendelijk zijn, dus we moeten niet overspoeld worden met gegevens. Het moet geconfigureerd kunnen worden a.d.h.v. templates. Het moet simpele opvolging hebben van events, dat je bijvoorbeeld events kunt afvinken.

10. Welke onderdelen van de infrastructuur worden momenteel geautomatiseerd bij Oosterberg?

De Citrix servers a.d.h.v. de Golden-image. Windows updates worden geautomatiseerd, deze gaan ook opnieuw opstarten. De virusscanner van TrendMicro is volledig geautomatiseerd, updates horen hier ook bij. Back-ups gaan automatisch d.m.v. Veeam, PRTG met het monitoren werkt nu ook geautomatiseerd. Het Hyper-V cluster melden zichzelf bij HP als er iets hardware-matig stuk gaat.

11. Zijn er nog dingen die jij graag ziet gebeuren in de loop of tijdens de afronding van dit project?

Het zou mooi zijn als we tijdens het proof of concept kunnen zien, dat we al meer grip krijgen op onze infrastructuur.

12.8 Bijlage 8: Interview - Systeembeheerder

Interviewvragen worden opgedeeld in organisatievragen en technische vragen. Door vanuit dezelfde interviewer, dezelfde vragen aan verschillende belanghebbenden te stellen, worden er verschillende antwoorden gegeven. De antwoorden blijven zo, voor zover mogelijk, betrouwbaar en valide.

Organisatievragen

1. In welke sector bevindt Oosterberg zich?

Groothandel, niet zo zeer industrie omdat we geen productie doen. Eigen CAO, elektrotechnische groothandel, dit is een vrij nieuwe.

2. Welke diensten en producten worden door Oosterberg geleverd en hoe wordt dit gedaan?

Elektrotechnisch installatiemateriaal, hier en daar ook op maat gemaakte diensten. Verhuur van magazijn aan kleine bedrijven. Baliecontacten, webshop, telefonisch, winkelklanten.

3. Hoe zou je de organisatie beoordelen met betrekking tot het naleven van eigen kernwaarden en zijn er punten die verbeterd worden?

Druk mee om na te leven, gaat tot nu toe goed. “we verkopen altijd een ja”, we hebben ook echt wel eens een nee. Onderscheid maken ten opzichte van concurrentie is belangrijk, oosterberg is een familiebedrijf.

4. Wat zijn de belangrijkste processen van de organisatie?

De orderstroom, dat je de voorraad die je verkoopt meteen op de stoep staat bij diegene.

5. Wat zijn mogelijke ICT-technische bedreigingen voor het bedrijf?

Diefstal van bedrijfsdata, het binnen halen van virussen, onderdeel zijn van een botnet. Bedrijfscontinuïteit is het belangrijkste voor Oosterberg en deze bedreigingen kunnen dit stopzetten.

6. Hoe is de dynamiek en werkverdeling binnen de ICT-afdeling?

Dynamiek is erg goed, automatisering loopt achter met de mankracht. Met name aan de systeembeheerkant. Een extra FTE zou geen kwaad kunnen.

7. Op welke gebieden zie jij zelf graag de ICT-afdeling en het ICT-landschap op positieve wijze wijzigen in de (nabije) toekomst?

We voeren momenteel grote verbeteringen door, door de implementatie van een nieuwe Citrix-desktopomgeving. De Topdesk vernieuwing kijk ik naar uit en ik zou meer netwerk willen hebben. Ik bedoel hiermee: op elke vestiging een wifi gasten netwerk, dit is nu nog niet. Er is momenteel te weinig bandbreedte. Tot slot ook het loslaten van printbeheer en dit nu onderzetten in een contract.

8. Bestaat er een beheerplan en hoe wordt deze nageleefd?

Dit wordt momenteel opgebouwd, er zit een goed tempo in. Momenteel hebben we hem dus nog niet rond.

Technische vragen

1. Wat is volgens jou de huidige status van logs- en events van infrastructuurcomponenten bij Oosterberg?

Er zijn eventviewers op elke server en er is sinds recent een syslog server. Deze is nog niet geoptimaliseerd en het is een vrij grote bulk van data. De data is er dus hier en daar al wel, maar het is nog niet proactief en we proberen nu steeds meer te analyseren.

2. Welke problemen komt Oosterberg tegen in relatie tot de status van de aanwezigheid van logs- en events?

Er is teveel data, teveel irrelevante data. We zullen dit eerst verder moeten inrichten.

3. Wat is de huidige manier van werken en beheer, als het gaat om het detecteren van een potentiële hacker of data lek?

Een tijd geleden was er een potentiële lek vanuit een van onze firewalls. Er is toen gesproken of we dit beter in kunnen zien. De documentatie hieromheen is ook nog niet inzichtelijk. We hebben sinds dien ook geautomatiseerde mailtjes wanneer er foutieve logins zijn op servers.

4. Is er een DLP-beleid en in hoeverre wordt deze nageleefd?

Dat durf ik niet te zeggen, geen idee. Het enige wat we momenteel doen is het dichtmaken van data en accounts op moment dat er iemand bijvoorbeeld op non-actief wordt gezet die werkte bij Oosterberg. Dit gaat niet via officiële wegen of documenten, zo wordt er alleen een kort (Teams) berichtje gestuurd.

5. Tot hoever kan Oosterberg (historische) data terugzien van infrastructuurcomponenten?

Geen idee, dit lijkt mij ook iets voor meer voor (nog) grotere bedrijven. Switch of Router data hebben we momenteel nog niet ingericht. De statische configuratie van de switches hebben we wel.

6. Wat zijn de primaire belangen bij het implementeren van een monitoringoplossing binnen Oosterberg?

De bedrijfscontinuïteit op een hoger niveau krijgen, je moet niet stilstaan door veiligheidsissues. Het voorkomen van diefstal van bedrijfsgegevens.

7. Zijn er bepaalde veiligheids- of back-up regels waar Oosterberg zich aan houdt die van belang kunnen zijn bij het project?

We hebben een Veeam back-up, retentiebeleid is van een paar dagen, maand en dan nog voor 1 jaar.

8. Staan er grote wijzigingen op de planning omtrent de netwerkcomponenten die Oosterberg momenteel heeft?

Een jaar of 2/3 geleden zijn er al veel switches bijgewerkt. De core-switches moeten wat mij betreft nog wel een keer bij worden. Die zijn ondertussen al bijna 9 jaar oud.

9. Wat zijn vanuit jou eisen waaraan een monitoringoplossing zich zou moet voldoen?

Vooral dat het werkbaar moet zijn, het hoeft niet eenvoudig te zijn maar je moet de data er wel goed uit kunnen halen. Je moet het met een paar klikken of geautomatiseerd kunnen doen, het liefst niet met een specialisme. Je moet dan wel iemand hebben die weet hoe het allemaal werkt. Beheers vriendelijk en intuïtief zijn begrippen die hier naar boven komen.

10. Welke onderdelen van de infrastructuur worden momenteel geautomatiseerd bij Oosterberg?

Wat mij zo te binnen schiet is de MDT-tool voor laptops en de Thin Clients worden met de HPDM server gedaan. Verder ook het opstarten van de Citrix server, een herstart of startup wordt direct geautomatiseerd gedaan via een golden-image. Voorheen was dit allemaal met de hand en koste het een lange tijd om op te zetten. De Windows updates worden ook gedaan naar alle domein-deelnemende apparatuur zoals laptops, krijgen allemaal via policies de updates binnen. De security updates krijgen ze ook via de trend client vanzelf binnen.

11. Zijn er nog dingen die jij graag ziet gebeuren in de loop of tijdens de afronding van dit project?

Nee, niets schiet mij zo te binnen.

12.9 Bijlage 9: Interview – ICT-Manager

Interviewvragen worden opgedeeld in organisatievragen en technische vragen. Door vanuit dezelfde interviewer, dezelfde vragen aan verschillende belanghebbenden te stellen, worden er verschillende antwoorden gegeven. De antwoorden blijven zo, voor zover mogelijk, betrouwbaar en valide.

Organisatievragen

1. In welke sector bevindt Oosterberg zich?

Groothandel, de elektrotechnische groothandel. De installateur en de w en de e tak, maar Oosterberg zit echt in de E, maar het schuurt dicht tegen W aan.

2. Wat is de marktpositie van Oosterberg?

Wij zijn de op 2 na grootste in deze sector, we zijn erg sterk groeiend. We snoepen veel van onze concurrenten af en we zitten in de markt met heel veel concurrenten. Maar er zijn eigenlijk 4 grote spelers, Technische Unie is bijvoorbeeld echt een stuk groter dan Oosterberg. Oosterberg zal rond de 10/ 15% markt aandeel zitten.

3. Wat is de strategie van Oosterberg?

Lastige vraag, een belangrijk kenmerk voor Oosterberg is, is dat wij erg anticiperen op wat er gebeurt. We gingen van piano handel, naar witgoed, naar de E-handel. Nu gaan we bijvoorbeeld erg naar Third party logistiscs (3PL).

4. Wat is de missie van Oosterberg?

Dit kan beter van de site opgehaald worden. Maar het is in ieder geval erg belangrijk dat er wederzijdse afhankelijkheid is tussen Oosterberg en de klant. Maar dit ook met de leveranciers en Oosterberg. Het onderhouden van relaties is belangrijk. De onafhankelijke rol is hier van belang, wij kunnen onafhankelijk adviseren.

5. Welke diensten en producten worden door Oosterberg geleverd en hoe wordt dit gedaan?

Elektrotechnische producten en alles wat er daarvan te krijgen is. Wij kunnen niet concurreren met onze producten, het gaat echt om het concurreren van de dienstverlening, dit doen we door IT-integraties en het automatiseren van het gehele proces van aanschaf tot implementatie. Ook op logistiek gebied doen we snelle leveringen op de bouw, nachtleveringen. Wij verkorten ook erg de levertijd door het aanleggen van voorraden en buffers.

6. Wat is het aantal klanten dat Oosterberg heeft?

In totaal zijn er 23940 klanten bekend, waarvan er 13080 echt actief zijn in de laatste jaren.

7. Bestaat er grote concurrentie in de sector van Oosterberg?

Ja, heel veel. Zie vraag 2.

8. Hoe zou je de organisatie beoordelen met betrekking tot het naleven van eigen kernwaarden en zijn er punten die verbeterd worden?

Kernwaarden zijn ontstaan vanuit het bestaan van Oosterberg, het moet identiek zijn aan wie Oosterberg is. Het is ontstaan vanuit onze eigen medewerkers. Het lastige hierin is het laten adopteren van deze cultuur aan al die nieuwe medewerkers met de grootte groei.

9. Wat zijn de belangrijkste processen van de organisatie?

Logistiek is vanuit systeemperspectief het belangrijkste onderdeel. Vanuit organisatieperspectief is misschien de verkoop wel het belangrijkst. Men verwacht dat wij steeds meer een IT-bedrijf gaan worden. Third party logistiscs (3PL) omtrent het koppelen van allerlei services speelt hier een grote rol in.

10. Wordt er veel samengewerkt met andere bedrijven? En hoe zit dit op gebied van ICT?

Ondanks de diverse en brede kennis op IT zijn wij een regie-IT afdeling, wij werken alleen maar samen met andere bedrijven. Dat houdt ook in dat wij niet altijd op alle onderdelen de gespecialiseerde IT-kennis hebben. Dit zal natuurlijk verschillen per project, onderdeel of onderwerp.

11. Hoeveel medewerkers heeft Oosterberg op haar hoofdlocatie, en hoeveel in totaal?

50 of 70 op hoofdlocatie, in totaal denk ik zo'n 400 ondertussen. Daarbij zo'n 250 kantoorwerkers met Office-licenties.

12. Hoe is de dynamiek en werkverdeling binnen de ICT-afdeling?

De dynamiek is wel erg groot, we hebben met veel veranderingen te maken. Wij staan dit niet uit de weg als bedrijf. De verdeling is momenteel infrastructuur en proces- en applicatiebeheer. Infrastructuur is nog iets minder verdeeld, maar proces- en applicatie zit al wel in DevOps-teams.

13. Op welke gebieden zie jij zelf graag de ICT-afdeling en het ICT-landschap op positieve wijze wijzigen in de (nabije) toekomst?

Aan de infra kant hoop ik dat we het beheer meer onder controle krijgen, het beheerplan bijvoorbeeld volledig inzetten met daarbij de uitvoering. Dat we de security-roadmap volledig af kunnen ronden. We moeten meer proactief en planmatig te werk gaan. Aan de applicatiekant wil ik meer naar de DevOps-teams en qua bezetting meer krijgen. Het grootste wat er nog aan zit te komen is het uitfaseren van onze ERP-oplossingen en het integreren van een nieuwe.

14. Bestaat er een beheerplan en hoe wordt deze nageleefd?

Nog niet, die is momenteel in ontwikkelingen.

15. Wat is de processtroom van ICT-ontwikkelingen richting de goedkeuring van het management?

Geen officiële processtroom, maar er is vaak een jaarplan waar we in het hele jaar kijken waar we ons op gaan richten. Vanuit daar vloeien allerlei projecten en die zoeken wij uit. Als dit grote en ingrijpende projecten zijn dan wordt er vanuit mij (manager) een voorstel ingediend aan MT.

16. Zijn er organisatorische tekeningen beschikbaar?

Ja, deze staan op het intranet beschikbaar gesteld vanuit KAMV.

Technische vragen

1. Bestaat er een overzicht/ tekening van het gehele ICT-landschap?

Zie applicatielandschap map op automatiseringsschijf, systeembeheer heb je al.

2. Bestaat er een architectuurtekening/ ontwerp van de infra, applicatie en business processen?

Nee deze is er niet.

3. Wat is het perspectief van de ICT-afdeling op gebruik van cloudapplicaties en/ of oplossingen?

Wij zijn niet tegenstander of voorstander van de cloud, wij zullen altijd blijven kijken naar wat het ons brengt. De onderbouwing is belangrijk voor de keuze, dit zullen wij per onderdeel en per project op deze manier doen.

4. Wat zijn gevaarlijkste ICT-technische bedreigingen voor het bedrijf?

Wat ik zelf als grootste gevaar zie is de cybercriminaliteit, hier gaat het echt om gijzelen. Dus de ransomware, dus de gijzelsoftware. Een tweede zou denk ik zijn het borgen van kennis over de systemen is echt iets belangrijks voor ons.

5. Wat is volgens jou de huidige status van logs- en events van infrastructuurcomponenten bij Oosterberg?

Daar hebben we eigenlijk weinig oog voor nu, niet echt bewust wat je er mee kan momenteel. Het gedeelte wat er is, is erg verspreid. We zijn niet in controle over die data die er is.

6. Welke problemen komt Oosterberg tegen in relatie tot de status van de aanwezigheid van logs- en events?

Dat we niet dingen proactief signaleren, niet kunnen signaleren. Dat we geen overkoepelende verbanden kunnen zien, geen trends kunnen inzien, geen analyses kunnen uitvoeren. We hebben geen forensisch materiaal, we kunnen niet zien dat er een hacker is geweest. Je ziet zo niet waar zo'n hacker is geweest en wat hij heeft gekregen.

7. Welke onderdelen van het ICT-landschap komt de AVG direct bij kijken?

We hebben niet echt onderdelen. We hebben een AVG-werktraject gehad, maar hoe actief die werkgroep is die daar bij hoort weet ik niet. We hebben in onze IT-omgeving weinig met persoonsgegevens te maken. PZ doet dit wel, maar de applicaties die zij gebruiken zijn cloud-based, wij zijn klanten van die partijen dus zij zijn in dit geval degenen die dan het AVG-beleid goed op moeten stellen.

8. Wat is de huidige manier van werken en beheer, als het gaat om het detecteren van een potentiële hacker of data lek?

Die is nog erg reactief. In mijn ogen zijn we daar niet goed op voorbereid, wat we laatst hebben gehad met Fox-IT is het forensisch onderzoek. Maar dit was snel klaar omdat we geen historische data hadden. We hebben nog geen vaste procedures voor en we bekijken alles echt op dat moment. We kunnen wel snel schakelen, maar het blijft reactief en er is geen handboek bij onze afdeling voor dit soort beheer. Als er een globaal potentiële data lek is, dan volgen wij het advies van het centraal cybersecuritybureau.

9. Is er een DLP-beleid en in hoeverre wordt deze nageleefd?

Nee deze is er niet.

10. Tot hoever kan Oosterberg (historische) data terugzien van infrastructuurcomponenten?

Niet meer dan een halve dag volgens mij. De Netscaler en o365 historie is er wel een stuk meer.

11. Wat zijn de primaire belangen bij het implementeren van een monitoringoplossing bij Oosterberg?

Dat we ons beter beveiligen op gebied van cybersecurity. Dat we die ransomware zien te voorkomen.

12. Zijn er bepaalde veiligheids- of back-up regels waar Oosterberg zich aan houdt die van belang kunnen zijn bij het project?

Niet zo zeer regels, maar wel het liefst dat het gescheiden wordt op basis van de bestaande machines etc.

13. Staan er grote wijzigingen op de planning omtrent de netwerkcomponenten die Oosterberg momenteel heeft?

Back-up hardening is momenteel een project wat gaande is. Uiteindelijk willen we ook de back-up buiten het domein plaatsen. En de coreswitches willen we tot slot ook gaan vervangen.

14. Wat zijn vanuit jou eisen waaraan een monitoringoplossing zich zou moeten voldoen?

- Hoelang moeten logs bewaard worden
- Tool dient goeie voorzieningen te hebben om te kunnen filteren en zoeken
- Eventherkenning, welke events komen wanneer voor
- Severity score a.d.h.v. events, belangrijke meldingen meer prio
- Systeemherkenning op basis van merk/ type, de tool moet weten dat het een HP core switch is
- Signaleringen moeten gedaan worden adhv templates, analyses moeten gedaan worden adhv templates
- Wat zijn best practices omtrent gebruik SIEM
- Waar wordt de log bewaard,
- Verschillen tussen Siem in de cloud of on premise
- Siem moet cloud en on prem logs op kunnen halen
- Ingebouwd managementsysteem- meldingen goed kunnen keuren
- Eventueel topdesk integratie
- Kunnen applicaties gelogd worden, kan er meer gelogd worden dan alleen de netwerkcomponenten. Fileshares van de fileserver VM.
- Trends moeten geanalyseerd kunnen worden

15. Welke onderdelen van de infrastructuur worden momenteel geautomatiseerd bij Oosterberg?

Dit kan René beter beantwoorden. (Infra lead)

16. Zijn er nog dingen die jij graag ziet gebeuren in de loop of tijdens de afronding van dit project?

Wat ik graag zie gebeuren is dat monitoring, zoals bijvoorbeeld het inzetten van SIEM, echt gaat bijdragen aan de veiligheid van ons systeem en dat wij het als afdeling ook goed gaan adopteren. Daarbij schiet mij ook een eis/wens te binnen. We moeten wel een geschikte partner hebben die ons kan helpen bij implementatie van tool, die support kan leveren en die ons vooral verder helpt met het beveiligen m.b.v. SIEM. Dus bij voorkeur een partij die ons hierin kan aanbevelen.

12.10 Bijlage 10: Interview – ICT-Directeur

Organisatievragen

1. Welke doelen stel jij voorop binnen de ICT-afdeling en omgeving?

Veiligheid, in de loop van de jaren schalen we meer op. ICT moet gewoon goed geregeld zijn nu, continuïteit en beschikbaarheid zijn belangrijk en kunnen onderverdeeld worden. Het is belangrijk dat wij genoeg kennis en kunde hebben om mee te kunnen discussiëren met onze leveranciers. Risicoanalyses kunnen uitvoeren is steeds belangrijker. Procesmatig werken is belangrijker, maar dit wordt nog niet genoeg gedaan. Ik vind het belangrijk om proceskennis over de hele organisatie te hebben. Infrastructuur moet meer kunnen werken in de vorm van een regie functie, de software en proceskant moet meer 80% in eigen huis hebben.

2. Welke rapportages ontvang jij/ of zou je graag willen ontvangen omtrent ICT?

KPI's zijn we aan het opzetten, maar bij IT is dit nog lastig. Trendanalyses staan centraal en ik denk dat wij hier het meeste uit kunnen halen en mee kunnen.

3. Welke primaire belangen heb jij zelf bij ICT-projecten?

Dit geldt niet alleen voor ICT, maar er moet meer project gericht gaan werken. Proceskant kan bijvoorbeeld beter, infrastructuur projectmatig werken gaat wel goed naar mijn idee.

4. Op welke gebieden zie jij zelf graag de ICT-afdeling en het ICT-landschap op positieve wijze wijzigen in de (nabije) toekomst?

Meer project en procesmatig gaan werken. De capaciteit op zowel uren als kennisniveau afstemmen op hetgeen wat van ons verwacht wordt.

5. Bestaat er een beheerplan en hoe wordt deze nageleefd?

Nee, in ontwikkeling op operationeel niveau.

6. Wat is de processtroom van ICT-ontwikkelingen richting de goedkeuring van het management?

Echt een goed jaarplan maken is de basis, deze is er al wel maar wordt niet volledig en juist besproken. Per project dat er aan de beurt is komt er een besluitstuk geschreven door de manager, waar risico's etc. instaan. Deze wordt goedgekeurd vanuit MT.

7. Bestaan er processen omtrent monitoren en het constateren van beveiligingslekken?

Nee, maar we zullen ergens de balans moeten vinden. We beschrijven vrij weinig in de organisatie maar processen zullen geborgd moeten worden.

Technische vragen

12. Bestaat er een architectuurtekening/ ontwerp van de infra, applicatie en business processen?

Netwerktekening van infrastructuur, informatie en processtroom van applicatie. Geen archi.

13. Wat is het perspectief van de ICT-afdeling op gebruik van cloudapplicaties en/ of oplossingen?

Geen cloud first strategie, maar we maken onderbouwde keuzes op basis van onderzoeken per onderdeel. Weloverwogen keuze tussen complexiteit, kosten en baten.

14. Welke problemen komt Oosterberg tegen in relatie tot de status van de aanwezigheid van logs- en events?

Naast de besproken algemene problemen aan het begin van het gesprek durf ik hier geen exact antwoord op te geven.

15. Bestaan er extra rollen in de ICT-organisatie, zoals een data protection officer?

Nee, dit zal er wel meer aankomen. Maar we hebben niet een goed beeld van welke belangen per afdeling of per IT onderdeel. Redundantie w.b.t. rollen zal belangrijk zijn.

16. Waarom wil Oosterberg een monitoringsvoorziening inzetten?

Alle drie maar vooral risico management.

- **a.** (compliance, risico management, governance)
  - **i.** Beleidslijnen en procedures, audit support, wet- en regelgeving
  - **ii.** Bescherming tegen dreigingen, incident respons, forensisch onderzoek, rechtszaken
  - **iii.** IT performance management, troubleshooting, IT-services op basis van SLA's

17. Staan er grote wijzigingen op de planning omtrent de processen binnen Oosterberg?

Heel veel proces wijzigen staan op de planning, transport is er een van. Hele structuur wordt daar omgegooid, warehousing, sales. IT alleen in de toekomst, maar nog niet op de huidige planning.

18. Staan er grote wijzigingen op de planning omtrent de netwerkcomponenten die Oosterberg momenteel heeft?

Een exact antwoord kan een systeembeheerder je beter geven denk ik.

19. Zijn er nog dingen die jij graag ziet gebeuren in de loop of tijdens de afronding van dit project?

Vervolgstappen inzichtelijk maken is belangrijk, ik wil graag dat we continu bezig zijn met het door ontwikkelen. Stilstaan kan gewoon niet.

Leiderschapsvragen

1. **Hoe zou jij de manier van leiddinggeven beschrijven bij Oosterberg en verschilt dit per afdeling?**

Ik denk dat de manier niet directief is, erg dichtbij de operatie is het wel. We veranderen hier wel in, we krijgen veel nieuwe mensen. Cultuur verschillen omtrent aanpak is hier een van de gevolgen door.

2. **Wat is jouw manier van leiddinggeven?**

Niet directief, graag samen met de mensen. Samenwerken is voor mij belangrijk, niet zo politiek gericht maar meer situationeel gericht.

3. **Welke vaardigheden heb je volgens jou nodig om leiding te kunnen geven?**

Sowieso ben ik van mening dat als je leiding wil geven dat je kennis moet hebben van het onderdeel waar je leiding over geeft. En vertrouwen uitstralen is belangrijk, maar dit moet wel over en weer gebeuren, coachend en situationeel leiderschap is belangrijk. Leiderschapsstijl aan kunnen passen is belangrijk. Je moet echt weten waar het over gaat, beslissingen nemen zonder kennis is funest.

4. **Hoe wil je dat er naar jou wordt gekeken als leidinggevende?**

Dat ze vertrouwen hebben, ondanks dat je af en toe duidelijk moet zijn.

5. **Geef je ook aan hoe er gecontroleerd wordt en op welke wijze er besluiten worden genomen?**

Het controleren zijn we niet heel goed in, maar het controleren mag wel ietsje meer gebeuren.

6. **Worden er gesprekken gevoerd met jouw personeel en zo ja, wat voor gesprekken zijn dit?**

Ik doe het met de manager, maar genoeg doen we dit niet. Verbeterpunten zijn het voeren van meer functioneringsgesprekken, of gewoon voortgangsgesprekken. Dit is misschien ook wel een verbeterpunt voor mezelf.

7. **Heb je inspiratiebronnen als leider?**

Niet een specifiek iemand, ik kijk meer naar mijn nabije omgeving. Naar andere directieleden, managers en zie wat er gebeurt in mijn eigen omgeving, je moet jezelf blijven.

8. **Wat zijn de leuke aspecten van leiderschap?**

Met elkaar dingen realiseren.

9. **Wat zijn de lastige aspecten van leiderschap?**

Politiek, een lastig ding is mensen die niet makkelijk coach baar zijn. Je ziet dan op tegen de gesprekken met die personen, maar wel erg fijn als je ze dan weer gehad hebt.

10. **Heb je afrondend nog tips over leiddinggeven?**

Het belangrijkste is dat je geen gedrag uitstraalt die niet bij je past. Je moet wel jezelf blijven, aangeleerd gedrag past niet bij de functie.

12.11 Bijlage 11: Interview – Infrastructuurbeheerder deel 2

Organisatievragen

1. Welke doelen stel jij voorop binnen de ICT-afdeling en omgeving?

Beveiliging, redundantie, stabiele performance

2. Welke rapportages ontvang jij/ of zou je graag willen ontvangen omtrent ICT?

Ontvang alle PRTG alerts, ontvang WSUS meldingen, Syslog meldingen en ILO meldingen. Alle melden komen via de mail binnen. Zijn meer meldingen dan rapportages. Password reset tool geeft een rapportage. WSUS geeft wel rapportages over welke computers er geüpdatet zijn of fouten hebben. De virusscanner TrendMicro geeft ook meldingen en rapportages.
In de toekomst zou ik de trends willen zien in de vorm van rapportages van bijvoorbeeld PRTG. Dit zijn nu meer meldingen.

3. Bestaan er processen omtrent monitoren en het constateren van beveiligingslekken?

De applicaties die meldingen en rapportages geven die bieden inzicht, hierop wordt actie ondernomen, maar zonder monitoringsproces. Er is wel een beheerplan in ontwikkeling.

Technische vragen

1. Bestaat er een architectuurtekening/ ontwerp van de infra, applicatie en business processen?

Nee. Wel van de ERP-omgeving.

2. Bestaan er extra rollen in de ICT-organisatie, zoals een data protection officer?

Nee. Ik vervul de taken een beetje maar dat is het.

3. Waarom wil Oosterberg een monitoringsvoorziening inzetten?

Risico Management, vooral door de bedreigingen en de forensische onderzoeken. We willen wel meer naar governance toe, omdat we dan beheersbaar maken wat we hebben. Door middel van procedures lopen we dan niet achter de feiten aan.

4. Staan er grote wijzigingen op de planning omtrent de processen binnen Oosterberg?

Het beheerplan zal grote wijzingen brengen in de werkwijzen binnen de IT-afdeling.

12.12 Bijlage 12: Interview – Manager-ICT deel 2

Organisatievragen

1. Welke doelen stel jij voorop binnen de ICT-afdeling en omgeving?

Continuïteit, beveiliging vloeit hier uit voort. Beveiliging doen we eigenlijk ook alleen om de continuïteit te waarborgen.

2. Welke rapportages ontvang jij/ of zou je graag willen ontvangen omtrent ICT?

Rapportages uit Topdesk over aantal meldingen. Geen rapportages op gebied van security. Nu hebben we Holm en PRTG waar rapportages uit kunnen komen. Rapportages over gedrag op het netwerk, vreemde logins, zaken die afwijken. Bij mij gaat het om de severity, het aantal kwetsbaarheden etc. Hoeveel er weggenomen worden is er bijvoorbeeld ook een. Die trendanalyses heb ik het dan over.

- Preventief: Zo dicht mogelijk
- Detectie: Mochten ze toch binnen zijn, wat gebeurt er dan

3. Bestaan er processen omtrent monitoren en het constateren van beveiligingslekken?

Nee

Technische vragen

1. Bestaan er extra rollen in de ICT-organisatie, zoals een data protection officer?

Nee.

2. Waarom wil Oosterberg een monitoringsvoorziening inzetten?

Voor Risico Management, we moeten forensisch onderzoek kunnen doen en we moeten ons kunnen beschermen. Processen mogen niet stil te komen liggen, dus beveiliging is daarom belangrijk. Vreemd gedrag kunnen herkennen. Interne beleidslijnen staat op de nice to have lijst, maar is niet primaire belang.

3. Staan er grote wijzigingen op de planning omtrent de processen binnen Oosterberg?

Nu nog niet, helemaal niet op basis van ICT-gebied. Applicatielandschap gaat richting Azure, dit gaat zich nog meer nestelen in de infrastructuur. Oosterberg gaat meer cloudbased werken. Dit moet dus ook allemaal in de monitoring staan.

Leiderschapsvragen

1. **Hoe zou jij de manier van leiddinggeven beschrijven bij Oosterberg en verschilt dit per afdeling?**

Informeel, niet hiërarchisch, meer als teamgenoot. Bij logistiek zal er meer hiërarchie zijn. Vanuit vroeger zat er al in dat er niet teveel gelaagdheid in de organisatie zat.

2. **Wat is jouw manier van leiddinggeven?**

Informeel, als teamgenoot. Niet hiërarchisch. Ik probeer het goede voorbeeld te zijn.

3. **Welke vaardigheden heb je volgens jou nodig om leiding te kunnen geven?**

Empathisch vermogen is belangrijk, goed moeten kunnen luisteren. Niet te bevooroordeeld moet zijn, je moet open staan voor dingen. Je moet niet voorop willen staan, niet altijd ten minste. Je moet volgens mij een steun zijn voor je medewerkers.

4. **Hoe wil je dat er naar jou wordt gekeken als leidinggevende?**

Dat iedereen mij vertrouwd, wantrouwen wil ik absoluut voorkomen. Dat collega's zich geholpen voelen, inhoudelijk bijvoorbeeld.

5. **Geef je ook aan hoe er gecontroleerd wordt en op welke wijze er besluiten worden genomen?**

Wij controleren niet op werk, dus we zijn minder gefocust op kwantiteit maar meer op kwaliteit. Maar het bijhouden waar iedereen mee bezig is doe ik wel.

6. **Worden er gesprekken gevoerd met jouw personeel en zo ja, wat voor gesprekken zijn dit?**

Veel werkoverleg, dus wel inhoudelijke gesprekken, projectgesprekken. De functioneringsgesprekken zijn er ook eenmaal per jaar. Informele gesprekken komen zo vanzelf binnen.

7. **Heb je inspiratiebronnen als leider?**

Ik verdiep me weinig in leiderschap, ik heb wel trainingen gehad met een privé coach binnen Oosterberg. Mocht ik toch een voorbeeld moeten noemen, dan is René Leisink (IT-directeur) wel een goed voorbeeld. Hij is volgens mij zo bijna de enige die dingen kan verwezenlijken, maar ook goed kan enthousiasmeren.

8. **Wat zijn de leuke aspecten van leiderschap?**

Wat ik het leukste vind is om met een team samen te werken. Het voortouw daar wel (of niet) kunnen nemen is leuk en het betrokken zijn vind ik fijn.

9. **Wat zijn de lastige aspecten van leiderschap?**

Het lastigste is toch wel het verantwoordelijkheidsgevoel. Bij IT zit er niemand meer boven ons, zo voelt het tenminste. Vooral dit in combinatie met incidenten of storingen ervaar ik als een last.

10. **Heb je afrondend nog tips over leiddinggeven?**

Lees het boek van Stephen Covey, dat is een hele beroemde en goeie. Deze is niet alleen voor leidinggeven, maar ook voor persoonlijke ontwikkeling.